Air Live®
www.airlive.com

SNMP-GSH2416

8+16 Pure Gigabit SNMP Managed Switch

Table of Contents

CAUTION ---- IV
ELECTRONIC EMISSION NOTICES ---- IV

CHAPTER 1. INTRODUCTION ---- 2

1-1. OVERVIEW OF SNMP-GSH2416 SNMP MANAGED GIGABIT SWITCH ---- 2
1-2. CHECKLIST ---- 4
1-3. FEATURES ---- 4
1-4. VIEW OF SNMP-GSH2416 SNMP MANAGED GIGABIT SWITCH ---- 6
1-4-1. User Interfaces on the Front Panel (Button, LEDs and Plugs) ---- 6
1-4-2. User Interfaces on the Rear Panel ---- 7
1-5. VIEW OF THE OPTIONAL MODULES ---- 8

CHAPTER 2. INSTALLATION ---- 9

2-1. STARTING SNMP-GSH2416 SNMP MANAGED GIGABIT SWITCH UP ---- 9
2-1-1. Hardware and Cable Installation ---- 9
2-1-2. Installing Chassis to a 19-Inch Wiring Closet Rail ---- 11
2-1-3. Cabling Requirements ---- 11
2-1-3-1. Cabling Requirements for TP Ports ---- 12
2-1-3-2. Cabling Requirements for 1000SX/LX SFP Module ---- 12
2-1-3-3. Switch Cascading in Topology ---- 13
2-1-4. Configuring the Management Agent of 8-Port TP + 16-Port SFP L2 Managed Gigabit Switch ---- 16
2-1-4-1. Configuring the Management Agent of 8-Port TP + 16-Port SFP L2 Managed Gigabit Switch through the Serial RS-232 Port ---- 17
2-1-4-2. Configuring the Management Agent of 8-Port TP + 16-Port SFP L2 Managed Gigabit Switch through the Ethernet Port ---- 19
2-1-5. IP Address Assignment ---- 20
2-2. TYPICAL APPLICATIONS ---- 25

CHAPTER 3. OPERATION OF WEB-BASED MANAGEMENT ---- 26

3-1. WEB MANAGEMENT HOME OVERVIEW ---- 28
3-1-1. System Information ---- 31
3-1-2. IP Configuration ---- 33
3-1-3. Time Configuration ---- 36
3-1-4. Account Configuration ---- 39
3-1-5. Management Policy ---- 40
3-1-6. Virtual Stack ---- 43
3-2. PORT CONFIGURATION ---- 46
3-2-1.Port Status ---- 46
3-2-2. Port Configuration ---- 52

3-2-3. Simple Counter ---- 54
3-2-4. Detail Counter ---- 56
3-3. MIRROR ---- 59
3-4. BANDWIDTH MANAGEMENT ---- 60
3-5. QOS(QUALITY OF SERVICE) CONFIGURATION ---- 62
3-6. SNMP CONFIGURATION ---- 72
3-7. IGMP SNOOPING ---- 74
3-8. MAX. PACKET LENGTH ---- 78
3-9. DHCP BOOT ---- 79
3-10. VLAN ---- 80
3-10-1. VLAN Mode ---- 80
3-10-2. Tag-based Group ---- 83
3-10-3. Port-based Group ---- 85
3-10-4. Tag Rule ---- 87
3-11. MAC TABLE ---- 89
3-12. GVRP CONFIGURATION ---- 96
3-13. STP CONFIGURATION ---- 102
3-13-1. STP Status ---- 102
3-13-2. STP Configuration ---- 104
3-13-3. STP Port Configuration ---- 106
3-14. TRUNKING CONFIGURATION ---- 109
3-15. 802.1X CONFIGURATION ---- 116
3-16. ALARM CONFIGURATION ---- 126
3-17. CONFIGURATION ---- 129
3-17-1. Save/Restore ---- 130
3-17-2. Config File ---- 135
3-18. DIAGNOSTICS ---- 136
3-19. TFTP SERVER ---- 139
3-20. LOG ---- 140
3-21. FIRMWARE UPGRADE ---- 142
3-22. REBOOT ---- 143
3-23. LOGOUT ---- 144

CHAPTER 4. OPERATION OF CLI MANAGEMENT ---- 145

4-1. CLI MANAGEMENT ---- 145
4-1-1. Login ---- 145
4-2. COMMANDS OF CLI ---- 147
4-2-1. Global Commands of CLI ---- 148
4-2-2. Local Commands of CLI ---- 154

CHAPTER 5. MAINTENANCE ---- 235

5-1. RESOLVING NO LINK CONDITION ---- 235
5-2. Q&A ---- 235

APPENDIX A TECHNICAL SPECIFICATIONS ---- 236

APPENDIX B NULL MODEM CABLE SPECIFICATIONS ---- 240

Caution

Circuit devices are sensitive to static electricity, which can damage their delicate electronics. Dry weather conditions or walking across a carpeted floor may cause you to acquire a static electrical charge.

To protect your device, always:

- Touch the metal chassis of your computer to ground the static electrical charge before you pick up the circuit device.
- Pick up the device by holding it on the left and right edges only.

Electronic Emission Notices

Federal Communications Commission (FCC) Statement

This equipment has been tested and found to comply with the limits for a class A computing device pursuant to Subpart J of part 15 of FCC Rules, which are designed to provide reasonable protection against such interference when operated in a commercial environment.

European Community (CE) Electromagnetic Compatibility Directive

This equipment has been tested and found to comply with the protection requirements of European Emission Standard EN55022/EN60555-2 and the Generic European Immunity Standard EN50082-1.

EMC:	EN55022(1988)/CISPR-22(1985)	class A
	EN60555-2(1995)	class A
	EN60555-3	
	IEC1000-4-2(1995)	4K V CD, 8KV, AD
	IEC1000-4-3(1995)	3V/m
	IEC1000-4-4(1995)	1KV – (power line), 0.5KV – (signal line)

About this user's manual

In this user's manual, it will not only tell you how to install and connect your network system but configure and monitor the SNMP-GSH2416 SNMP Managed Gigabit Switch through the built-in CLI and web by RS-232 serial interface and Ethernet ports step-by-step. Many explanation in detail of hardware and software functions are shown as well as the examples of the operation for web-based interface and command-line interface (CLI).

Overview of this user's manual

- Chapter 1 "Introduction" describes the features of SNMP-GSH2416 SNMP Managed Gigabit Switch
- Chapter 2 "Installation"
- Chapter 3 "Operation of Web-based Management"
- Chapter 4 "Operation of CLI Management"
- Chapter 5 "Maintenance"

1. Introduction

1-1. Overview of SNMP-GSH2416 SNMP Managed Gigabit Switch

24-port Gigabit L2 Managed Switch, is a standard switch that meets all IEEE 802.3/u/x/z Gigabit, Fast Ethernet specifications. The switch included 8-Port 10/100/1000Mbps TP and 16-Port Gigabit SFP Fiber management Ethernet switch. The switch can be managed through RS-232 serial port via directly connection, or through Ethernet port using CLI or Web-based management unit, associated with SNMP agent. With the SNMP agent, the network administrator can logon the switch to monitor, configure and control each port's activity in a friendly way. The overall network management is enhanced and the network efficiency is also improved to accommodate high bandwidth applications. In addition, the switch features comprehensive and useful function such as QoS (Quality of Service), Spanning Tree, VLAN, Port Trunking, Bandwidth Control, Port Security, SNMP/RMON, IGMP Snooping capability via the intelligent software. It is suitable for both metro-LAN and office application.

In this switch, 1000Mbps SFP Fiber transceiver is used for high-speed connection expansion.

- 1000Mbps LC, Multi-Mode, SFP Fiber transceiver
- 1000Mbps LC, 10km, SFP Fiber transceiver
- 1000Mbps LC, 30km, SFP Fiber transceiver
- 1000Mbps LC, 50km, SFP Fiber transceiver
- 1000Mbps BiDi LC, 20km, 1550nm SFP Fiber WDM transceiver
- 1000Mbps BiDi LC, 20km, 1310nm SFP Fiber WDM transceiver

10/100/1000Mbps TP is a standard Ethernet port that meets all IEEE 802.3/u/x/z Gigabit, Fast Ethernet specifications. 1000Mbps SFP Fiber transceiver is a Gigabit Ethernet port that fully complies with all IEEE 802.3z and 1000Base-SX/LX standards.

1000Mbps Single Fiber WDM (BiDi) transceiver is designed with an optic Wavelength Division Multiplexing (WDM) technology that transports bi-directional full duplex signal over a single fiber simultaneously.

For upgrading firmware, please refer to the Section 3-21 or Section 4-2-2 for more details. The switch will not stop operating while upgrading firmware and after that, the configuration keeps unchanged.

- **Key Features in the Device**

QoS:

Support Quality of Service by the IEEE 802.1P standard. There are two priority queue and packet transmission schedule.

Spanning Tree:

Support IEEE 802.1D, IEEE 802.1w (RSTP: Rapid Spanning Tree Protocol) standards.

VLAN:

Support Port-based VLAN and IEEE802.1Q Tag VLAN. Support 256 active VLANs and VLAN ID 1~4094.

Port Trunking:

Support static port trunking and port trunking with IEEE 802.3ad LACP.

Bandwidth Control:

Support ingress and egress per port bandwidth control.

Port Security:

Support allowed, denied forwarding and port security with MAC address.

SNMP/RMON:

SNMP agent and RMON MIB. In the device, SNMP agent is a client software which is operating over SNMP protocol used to receive the command from SNMP manager (server site) and echo the corresponded data, i.e. MIB object. Besides, SNMP agent will actively issue TRAP information when happened.

RMON is the abbreviation of Remote Network Monitoring and is a branch of the SNMP MIB.

The device supports MIB-2 (RFC 1213), Bridge MIB (RFC 1493), RMON MIB (RFC 1757)-statistics Group 1,2,3,9, VLAN MIB (802.1Q, RFC2674), Ethernet MIB (RFC 1643) and so on.

IGMP Snooping:

Support IGMP version 2 (RFC 2236): The function IGMP snooping is used to establish the multicast groups to forward the multicast packet to the member ports, and, in nature, avoid wasting the bandwidth while IP multicast packets are running over the network.

1-2. Checklist

Before you start installing the switch, verify that the package contains the following:

— A set of SNMP-GSH2416 SNMP Managed Gigabit Switch
— Modules (optional)
— Mounting Accessory (for 19” Rack Shelf)
— This User's Manual in CD-ROM
— AC Power Cord
— RS-232 Cable

Please notify your sales representative immediately if any of the aforementioned items is missing or damaged.

1-3. Features

The SNMP-GSH2416 SNMP Managed Gigabit Switch, a standalone off-the-shelf switch, provides the comprehensive features listed below for users to perform system network administration and efficiently and securely serve your network.

- **Hardware**
  - 8 10/100/1000Mbps Auto-negotiation Gigabit Ethernet TP ports
  - 16 1000Mbps SFP fiber ports
  - 400KB on-chip frame buffer
  - Jumbo frame support
  - Programmable classifier for QoS (Layer 4/Multimedia)
  - 8K MAC address and 4K VLAN support (IEEE802.1Q)
  - Per-port shaping, policing, and Broadcast Storm Control
  - IEEE802.1Q-in-Q nested VLAN support
  - Full-duplex flow control (IEEE802.3x) and half-duplex backpressure
  - Extensive front-panel diagnostic LEDs; System: Power, TP Port1-8: LINK/ACT, SPEED, SFP Port 9-24: SFP(LINK/ACT)

- **Management**
  - Supports concisely the status of port and easily port configuration
  - Supports per port traffic monitoring counters
  - Supports a snapshot of the system Information when you login
  - Supports port mirror function
  - Supports the static trunk function

- Supports 802.1Q VLAN
- Supports user management and limits three users to login
- Maximal packet length can be up to 9216 bytes for jumbo frame application
- Supports DHCP Broadcasting Suppression to avoid network suspended or crashed
- Supports to send the trap event while monitored events happened
- Supports default configuration which can be restored to overwrite the current configuration which is working on via web browser and CLI
- Supports on-line plug/unplug SFP modules
- Supports Quality of Service (QoS) for real time applications based on the information taken from Layer 2 to Layer 4, such as VoIP
- Built-in web-based management and CLI management, providing a more convenient UI for the user
- Supports port mirror function with ingress traffic
- Supports rapid spanning tree (802.1w RSTP)
- Supports 802.1X port security on a VLAN
- Supports user management and only first login administrator can configure the device. The rest of users can only view the switch
- SNMP access can be disabled and prevent from illegal SNMP access
- Supports Ingress, Non-unicast and Egress Bandwidth rating management with a resolution of 1Mbps
- The trap event and alarm message can be transferred via e-mail and mobile phone short message
- Supports diagnostics to let administrator knowing the hardware status
- Supports external loopback test to check if the link is ok
- TFTP for firmware upgrade, system log upload and config file import/export
- Supports remote boot the device through user interface and SNMP
- Supports network time synchronization and daylight saving
- Supports 120 event log records in the main memory and display on the local console

1-4. View of SNMP-GSH2416 SNMP Managed Gigabit Switch

Fig. 1-1 Full View of 8-Port TP + 16-Port SFP L2 Managed Gigabit Switch

1-4-1. User Interfaces on the Front Panel (Button, LEDs and Plugs)

There are 8 TP Gigabit Ethernet ports and 16 SFP fiber ports for optional removable modules on the front panel of the switch. LED display area, locating on the left side of the panel, contains a Power LED, which indicates the power status and 24 ports working status of the switch.

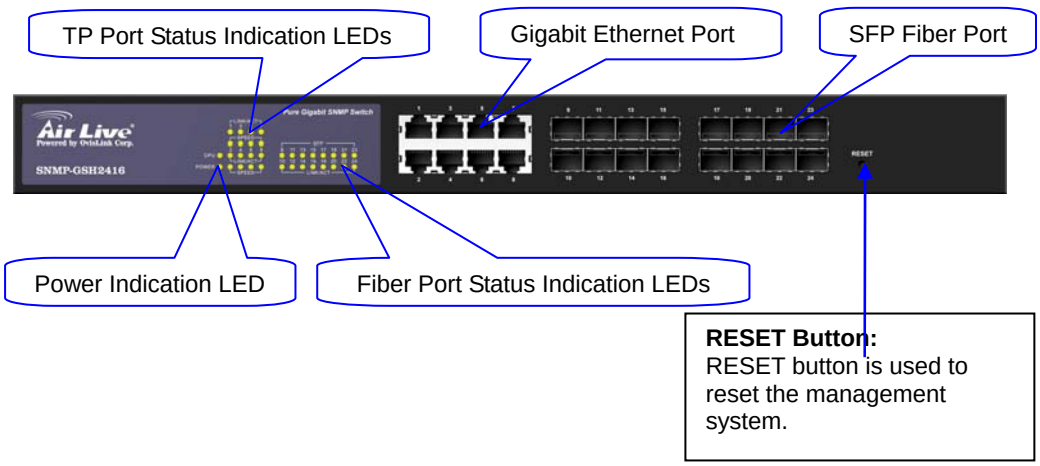


Fig. 1-2 Front View of 8-Port TP + 16-Port SFP L2 Managed Gigabit Switch

- **LED Indicators**

LED	Color	Function
System LED		
POWER	Green	Lit when +5V DC power is on and good
CPU LED	Green	Blinks when CPU is activity
10/100/1000Ethernet TP Port 1 to 8 LED		
LINK/ACT	Green	Lit when connection with remote device is good Blinks when any traffic is present Off when cable connection is not good
SPEED	Green/ Ember	Lit green when 1000Mbps speed is active Lit ember when 100Mbps speed is active Off when 10Mbps speed is active
1000SX/LX Gigabit Fiber Port 9 to 24 LED		
SFP(LINK/ACT)	Green	Lit when connection with the remote device is good Blinks when any traffic is present Off when module connection is not good

Table1-1

1-4-2. User Interfaces on the Rear Panel

One RS-232 DB-9 interface is offered for configuration or management.

Fig. 1-3 Rear View of 8-Port TP + 16-Port SFP L2 Managed Gigabit Switch

1-5. View of the Optional Modules

In the switch,1000Mbps SFP Fiber transceiver is used for high-speed connection expansion; the following are optional SFP types provided for the switch:

- 1000Mbps LC, MM, SFP Fiber transceiver (SFP.0LC.202)
- 1000Mbps LC, SM 10km, SFP Fiber transceiver (SFP.0LC.212.10)
- 1000Mbps LC, SM 30km, SFP Fiber transceiver (SFP.0LC.212.30)
- 1000Mbps LC, SM 50km, SFP Fiber transceiver (SFP.0LC.212.50)
- 1000Mbps BiDi LC, type 1, SM 20km, SFP Fiber WDM transceiver (SFP.0BL.621.201)
- 1000Mbps BiDi LC, type 2, SM 20km, SFP Fiber WDM transceiver (SFP.0BL.621.202)
- 1000Mbps LC, SM 10km, SFP Fiber transceiver with DDM (SFP.DLC.212.10)

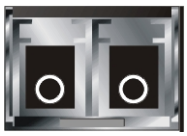


Fig. 1-4 Front View of 1000Base-SX/LX LC, SFP Fiber Transceiver

Fig. 1-5 Front View of 1000Base-LX BiDi LC, SFP Fiber Transceiver

2. Installation

2-1. Starting SNMP-GSH2416 SNMP Managed Gigabit Switch Up

This section will give users a quick start for:

- Hardware and Cable Installation
- Management Station Installation
- Software booting and configuration

2-1-1. Hardware and Cable Installation

At the beginning, please do first:

⇒ Wear a grounding device to avoid the damage from electrostatic discharge

⇒ Be sure that power switch is OFF before you insert the power cord to power source

- **Installing Optional SFP Fiber Transceivers to the Switch**

Note: If you have no modules, please skip this section.

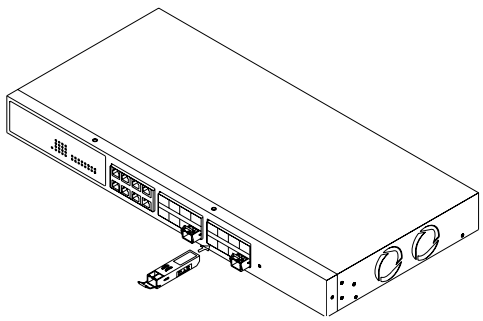


Fig. 2-1 Installation of Optional SFP Fiber Transceiver

- **Connecting the SFP Module to the Chassis:**

The optional SFP modules are hot swappable, so you can plug or unplug it before or after powering on.

1. Verify that the SFP module is the right model and conforms to the chassis
2. Slide the module along the slot. Also be sure that the module is properly seated against the slot socket/connector
3. Install the media cable for network connection
4. Repeat the above steps, as needed, for each module to be installed into slot(s)
5. Have the power ON after the above procedures are done

- **TP Port and Cable Installation**

⇒ In the switch, TP port supports MDI/MDI-X auto-crossover, so both types of cable, straight-through (Cable pin-outs for RJ-45 jack 1, 2, 3, 6 to 1, 2, 3, 6 in 10/100M TP; 1, 2, 3, 4, 5, 6, 7, 8 to 1, 2, 3, 4, 5, 6, 7, 8 in Gigabit TP) and crossed-over (Cable pin-outs for RJ-45 jack 1, 2, 3, 6 to 3, 6, 1, 2) can be used. It means you do not have to tell from them, just plug it.

⇒ Use Cat. 5 grade RJ-45 TP cable to connect to a TP port of the switch and the other end is connected to a network-aware device such as a workstation or a server.

⇒ Repeat the above steps, as needed, for each RJ-45 port to be connected to a Gigabit 10/100/1000 TP device.

Now, you can start having the switch in operation.

- **Power On**

The switch supports 100-240 VAC, 50-60 Hz power supply. The power supply will automatically convert the local AC power source to DC power. It does not matter whether any connection plugged into the switch or not when power on, even modules as well. After the power is on, all LED indicators will light up immediately and then all off except the power LED still keeps on. This represents a reset of the system.

- **Firmware Loading**

After resetting, the bootloader will load the firmware into the memory. It will take about 30 seconds, after that, the switch will flash all the LED once and automatically performs self-test and is in ready state.

2-1-2. Installing Chassis to a 19-Inch Wiring Closet Rail

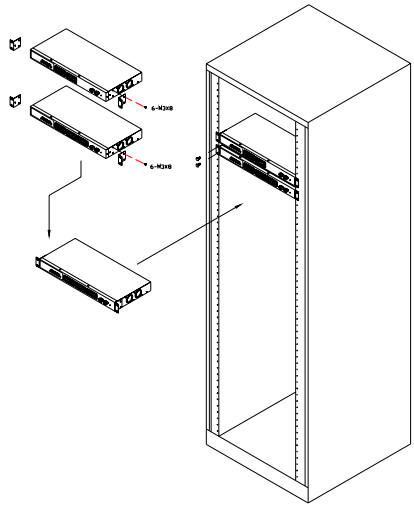


Fig. 2-2

Caution: Allow a proper spacing and proper air ventilation for the cooling fan at both sides of the chassis.

⇒ Wear a grounding device for electrostatic discharge.
⇒ Screw the mounting accessory to the front side of the switch (See Fig. 2-2).
⇒ Place the Chassis into the 19-inch wiring closet rail and locate it at the proper position. Then, fix the Chassis by screwing it.

2-1-3. Cabling Requirements

To help ensure a successful installation and keep the network performance good, please take a care on the cabling requirement. Cables with worse specification will render the LAN to work poorly.

2-1-3-1. Cabling Requirements for TP Ports

⇒ For Fast Ethernet TP network connection
- The grade of the cable must be Cat. 5 or Cat. 5e with a maximum length of 100 meters.

⇒ Gigabit Ethernet TP network connection
- The grade of the cable must be Cat. 5 or Cat. 5e with a maximum length of 100 meters. Cat. 5e is recommended.

2-1-3-2. Cabling Requirements for 1000SX/LX SFP Module

It is more complex and comprehensive contrast to TP cabling in the fiber media. Basically, there are two categories of fiber, multi mode (MM) and single mode (SM). The later is categorized into several classes by the distance it supports. They are SX, LX, LHX, XD, and ZX. From the viewpoint of connector type, there mainly are LC and BIDI LC.

- Gigabit Fiber with multi-mode LC SFP module
- Gigabit Fiber with single-mode LC SFP module
- Gigabit Fiber with BiDi LC 1310nm SFP module
- Gigabit Fiber with BiDi LC 1550nm SFP module

The following table lists the types of fiber that we support and those else not listed here are available upon request.

<table>
<tr><td rowspan="4">IEEE 802.3z Gigabit Ethernet 1000SX 850nm</td><td colspan="4">Multi-mode Fiber Cable and Modal Bandwidth</td></tr>
<tr><td colspan="2">Multi-mode 62.5/125μm</td><td colspan="2">Multi-mode 50/125μm</td></tr>
<tr><td>Modal Bandwidth</td><td>Distance</td><td>Modal Bandwidth</td><td>Distance</td></tr>
<tr><td>160MHz-Km</td><td>220m</td><td>400MHz-Km</td><td>500m</td></tr>
<tr><td>200MHz-Km</td><td>275m</td><td>500MHz-Km</td><td>550m</td></tr>
<tr><td rowspan="3">1000Base-LX/LHX/XD/ZX</td><td colspan="4">Single-mode Fiber 9/125μm</td></tr>
<tr><td colspan="4">Single-mode transceiver 1310nm 10Km</td></tr>
<tr><td colspan="4">Single-mode transceiver 1550nm 30, 50Km</td></tr>
<tr><td rowspan="4">1000Base-LX Single Fiber (BIDI LC)</td><td colspan="2" rowspan="2">Single-Mode *20Km</td><td>TX(Transmit) 1310nm</td><td></td></tr>
<tr><td>RX(Receive) 1550nm</td><td></td></tr>
<tr><td colspan="2" rowspan="2">Single-Mode *20Km</td><td>TX(Transmit) 1550nm</td><td></td></tr>
<tr><td>RX(Receive) 1310nm</td><td></td></tr>
</table>

Table2-1

2-1-3-3. Switch Cascading in Topology

- **Takes the Delay Time into Account**

Theoretically, the switch partitions the collision domain for each port in switch cascading that you may up-link the switches unlimitedly. In practice, the network extension (cascading levels & overall diameter) must follow the constraint of the IEEE 802.3/802.3u/802.3z and other 802.1 series protocol specifications, in which the limitations are the timing requirement from physical signals defined by 802.3 series specification of Media Access Control (MAC) and PHY, and timer from some OSI layer 2 protocols such as 802.1d, 802.1q, LACP and so on.

The fiber, TP cables and devices' bit-time delay (round trip) are as follows:

1000Base-X TP, Fiber		100Base-TX TP		100Base-FX Fiber	
Round trip Delay: 4096		Round trip Delay: 512			
Cat. 5 TP Wire:	11.12/m	Cat. 5 TP Wire:	1.12/m	Fiber Cable:	1.0/m
Fiber Cable :	10.10/m	TP to fiber Converter: 56			
Bit Time unit : 1ns (1sec./1000 Mega bit)		Bit Time unit: 0.01μs (1sec./100 Mega bit)			

Table 2-2

Sum up all elements' bit-time delay and the overall bit-time delay of wires/devices must be within Round Trip Delay (bit times) in a half-duplex network segment (collision domain). For full-duplex operation, this will not be applied. You may use the TP-Fiber module to extend the TP node distance over fiber optic and provide the long haul connection.

- **Typical Network Topology in Deployment**

A hierarchical network with minimum levels of switch may reduce the timing delay between server and client station. Basically, with this approach, it will minimize the number of switches in any one path; will lower the possibility of network loop and will improve network efficiency. If more than two switches are connected in the same network, select one switch as Level 1 switch and connect all other switches to it at Level 2. Server/Host is recommended to connect to the Level 1 switch. This is general if no VLAN or other special requirements are applied.

Case1: All switch ports are in the same local area network. Every port can access each other (See Fig. 2-3).

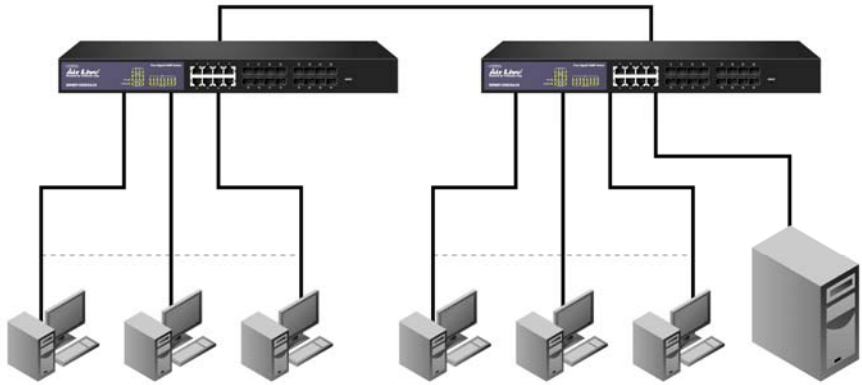


Fig. 2-3 No VLAN Configuration Diagram

If VLAN is enabled and configured, each node in the network that can communicate each other directly is bounded in the same VLAN area.

Here VLAN area is defined by what VLAN you are using. The switch supports both port-based VLAN and tag-based VLAN. They are different in practical deployment, especially in physical location. The following diagram shows how it works and what the difference they are.

Case2a: Port-based VLAN (See Fig.2-4).

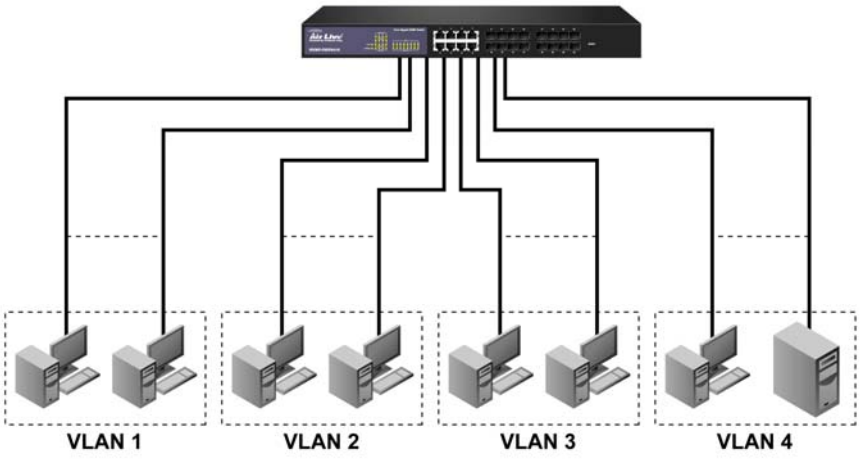


Fig. 2-4 Port-based VLAN Diagram

1. The same VLAN members could not be in different switches.
2. Every VLAN members could not access VLAN members each other.
3. The switch manager has to assign different names for each VLAN groups at one switch.

Case 2b: Port-based VLAN (See Fig.2-5).

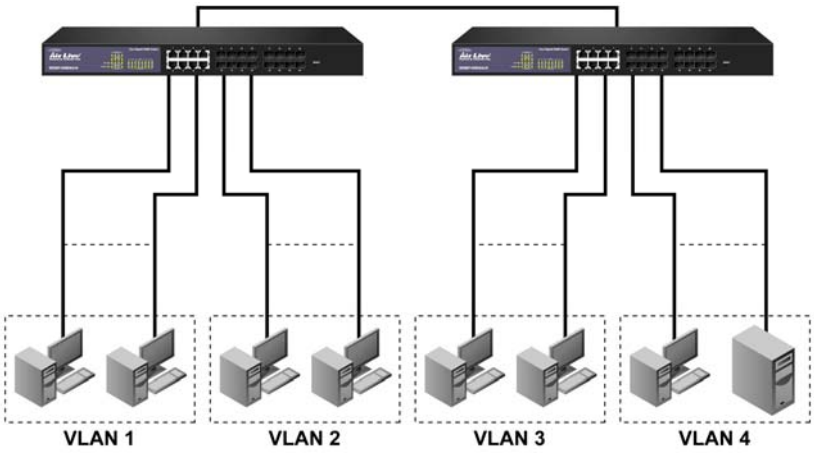
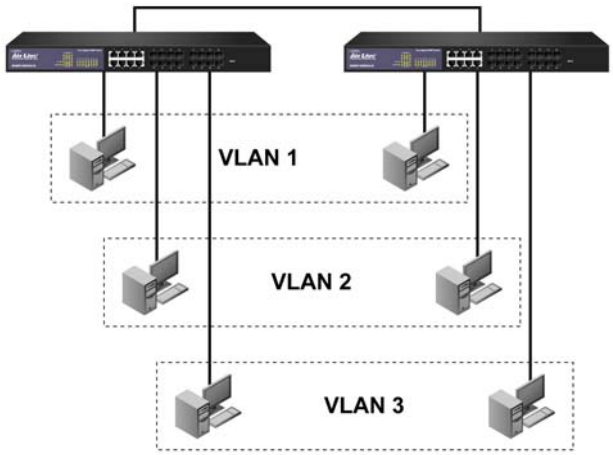


Fig. 2-5 Port-based VLAN Diagram

1. VLAN1 members could not access VLAN2, VLAN3 and VLAN4 members.
2. VLAN2 members could not access VLAN1 and VLAN3 members, but they could access VLAN4 members.
3. VLAN3 members could not access VLAN1, VLAN2 and VLAN4.
4. VLAN4 members could not access VLAN1 and VLAN3 members, but they could access VLAN2 members.

Case3a: The same VLAN members can be at different switches with the same VID (See Fig. 2-6).



2-1-4. Configuring the Management Agent of SNMP-GSH2416 SNMP Managed Gigabit Switch

We offer you three ways to startup the switch management function. They are RS-232 console, CLI, and Web. Users can use any one of them to monitor and configure the switch. You can touch them through the following procedures.

Section 2-1-4-1: Configuring the Management Agent of SNMP-GSH2416 SNMP Managed Gigabit Switch through the Serial RS-232 Port

Section 2-1-4-2: Configuring the Management Agent of SNMP-GSH2416 SNMP Managed Gigabit Switch through the Ethernet Port

Note: Please first modify the IP address, Subnet mask, Default gateway and DNS through RS-232 console, and then do the next.

2-1-4-1. Configuring the Management Agent of SNMP-GSH2416 SNMP Managed Gigabit Switch through the Serial RS-232 Port

To perform the configuration through RS-232 console port, the switch's serial port must be directly connected to a DCE device, for example, a PC, through RS-232 cable with DB-9 connector. Next, run a terminal emulator with the default setting of the switch's serial port. With this, you can communicate with the switch.

In the switch, RS-232 interface only supports baud rate 57.6k bps with 8 data bits, 1 stop bit, no parity check and no flow control.

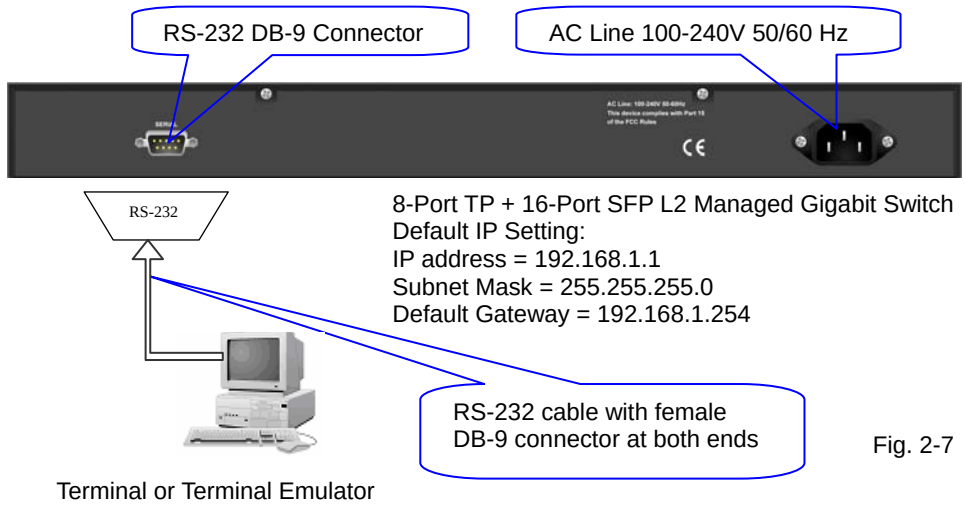

RS-232 DB-9 Connector
AC Line 100-240V 50/60 Hz
RS-232
8-Port TP + 16-Port SFP L2 Managed Gigabit Switch
Default IP Setting:
IP address = 192.168.1.1
Subnet Mask = 255.255.255.0
Default Gateway = 192.168.1.254
RS-232 cable with female
DB-9 connector at both ends
Terminal or Terminal Emulator

Fig. 2-7

To configure the switch, please follow the procedures below:

1. Find the RS-232 DB-9 cable with female DB-9 connector bundled. Normally, it just uses pins 2, 3 and 7. See also Appendix B for more details on Null Modem Cable Specifications.
2. Attaches the DB-9 female cable connector to the male serial RS-232 DB-9 connector on the switch.
3. Attaches the other end of the serial RS-232 DB-9 cable to PC's serial port, running a terminal emulator supporting VT100/ANSI terminal with The switch's serial port default settings. For example, Windows98/2000/XP HyperTerminal utility.

Note: The switch's serial port default settings are listed as follows:

Baud rate	57600
Stop bits	1
Data bits	8
Parity	N
Flow control	none

4. When you complete the connection, then press **<Enter>** key. The login prompt will be shown on the screen. The default username and password are shown as below:

Username = admin Password = admin

- **Set IP Address, Subnet Mask and Default Gateway IP Address**

Please refer to Fig. 2-7 CLI Management for details about the ex-factory setting. They are default setting of IP address. You can first either configure your PC IP address or change IP address of the switch, next to change the IP address of default gateway and subnet mask.

For example, your network address is 10.1.1.0, and subnet mask is 255.255.255.0. You can change the switch's default IP address 192.168.1.1 to 10.1.1.1 and set the subnet mask to be 255.255.255.0. Then, choose your default gateway, may be it is 10.1.1.254.

Default Value	SNMP-GSH2416 SNMP Managed Gigabit Switch	Your Network Setting
IP Address	192.168.1.1	10.1.1.1
Subnet	255.255.255.0	255.255.255.0
Default Gateway	192.168.1.254	10.1.1.254

Table 2-3

After completing these settings in the switch, it will reboot to have the configuration taken effect. After this step, you can operate the management through the network, no matter it is from a web browser or Network Management System (NMS).

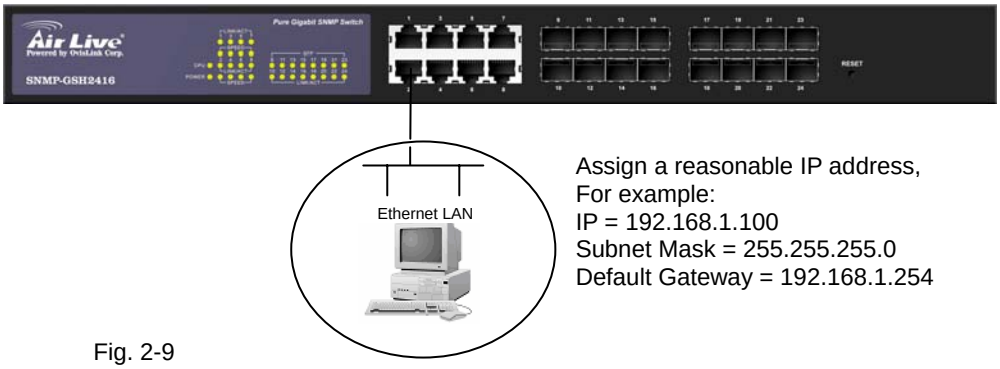
```
L2 Managed Switch - SNMP-GSH2416

Login: admin
Password:

SNMP-GSH2416#
```

Fig. 2-8 the Login Screen for CLI

2-1-4-2. Configuring the Management Agent of SNMP-GSH2416 SNMP Managed Gigabit Switch through the Ethernet Port

There are three ways to configure and monitor the switch through the switch's Ethernet port. They are CLI, Web browser and SNMP manager. The user interface for the last one is NMS dependent and does not cover here. We just introduce the first two types of management interface.

8-Port TP + 16-Port SFP L2 Managed Gigabit Switch
Default IP Setting:
IP = 192.168.1.1
Subnet Mask = 255.255.255.0
Default Gateway = 192.168.1.254



Assign a reasonable IP address,
For example:
IP = 192.168.1.100
Subnet Mask = 255.255.255.0
Default Gateway = 192.168.1.254

Fig. 2-9

- **Managing SNMP-GSH2416 SNMP Managed Gigabit Switch through Ethernet Port**

Before you communicate with the switch, you have to finish first the configuration of the IP address or to know the IP address of the switch. Then, follow the procedures listed below.

1. Set up a physical path between the configured the switch and a PC by a qualified UTP Cat. 5 cable with RJ-45 connector.

   Note: If PC directly connects to the switch, you have to setup the same subnet mask between them. But, subnet mask may be different for the PC in the remote site. Please refer to Fig. 2-9 about the switch's default IP address information.

2. Run CLI or web browser and follow the menu. Please refer to Chapter 3 and Chapter 4.

Fig. 2-10 the Login Screen for Web

2-1-5. IP Address Assignment

For IP address configuration, there are three parameters needed to be filled in. They are IP address, Subnet Mask, Default Gateway and DNS.

IP address:

The address of the network device in the network is used for internetworking communication. Its address structure looks is shown in the Fig. 2-11. It is “classful” because it is split into predefined address classes or categories.

Each class has its own network range between the network identifier and host identifier in the 32 bits address. Each IP address comprises two parts: network identifier (address) and host identifier (address). The former indicates the network where the addressed host resides, and the latter indicates the individual host in the network which the address of host refers to. And the host identifier must be unique in the same LAN. Here the term of IP address we used is version 4, known as IPv4.

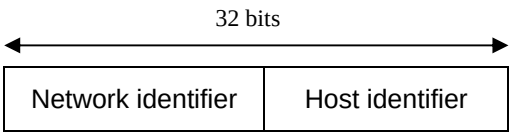
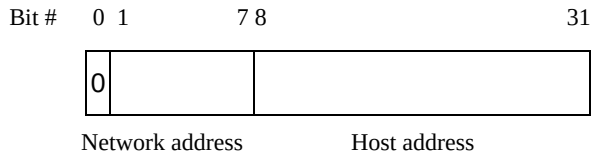


Fig. 2-11 IP address structure

With the classful addressing, it divides IP address into three classes, class A, class B and class C. The rest of IP addresses are for multicast and broadcast. The bit length of the network prefix is the same as that of the subnet mask and is denoted as IP address/X, for example, 192.168.1.0/24. Each class has its address range described below.

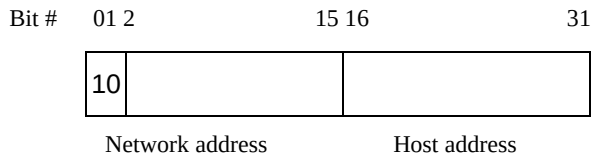
Class A:

Address is less than 126.255.255.255. There are a total of 126 networks can be defined because the address 0.0.0.0 is reserved for default route and 127.0.0.0/8 is reserved for loopback function.



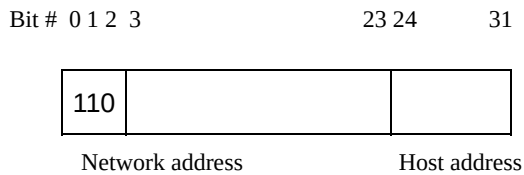
Class B:

IP address range between 128.0.0.0 and 191.255.255.255. Each class B network has a 16-bit network prefix followed 16-bit host address. There are 16,384 (2^14)/16 networks able to be defined with a maximum of 65534 (2^16 –2) hosts per network.



Class C:

IP address range between 192.0.0.0 and 223.255.255.255. Each class C network has a 24-bit network prefix followed 8-bit host address. There are 2,097,152 (2^21)/24 networks able to be defined with a maximum of 254 (2^8 –2) hosts per network.



Class D and E:

Class D is a class with first 4 MSB (Most significance bit) set to 1-1-1-0 and is used for IP Multicast. See also RFC 1112. Class E is a class with first 4 MSB set to 1-1-1-1 and is used for IP broadcast.

According to IANA (Internet Assigned Numbers Authority), there are three specific IP address blocks reserved and able to be used for extending internal network. We call it Private IP address and list below:

Class A	10.0.0.0 --- 10.255.255.255
Class B	172.16.0.0 --- 172.31.255.255
Class C	192.168.0.0 --- 192.168.255.255

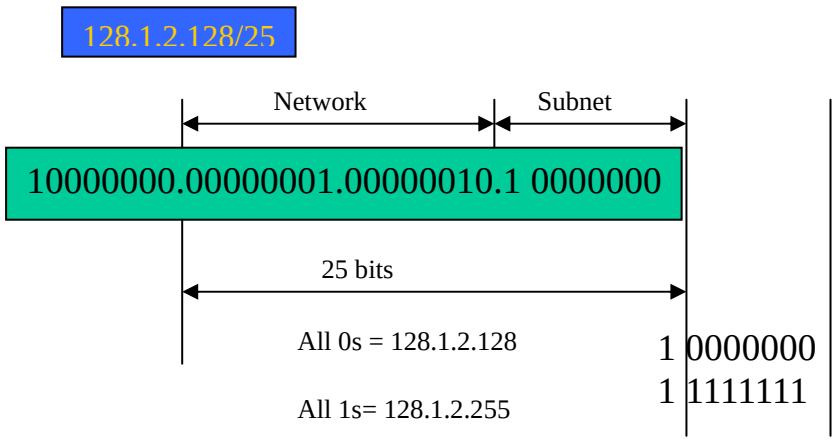
Please refer to RFC 1597 and RFC 1466 for more information.

Subnet mask:

It means the sub-division of a class-based network or a CIDR block. The subnet is used to determine how to split an IP address to the network prefix and the host address in bitwise basis. It is designed to utilize IP address more efficiently and ease to manage IP network.

For a class B network, 128.1.2.3, it may have a subnet mask 255.255.0.0 in default, in which the first two bytes is with all 1s. This means more than 60 thousands of nodes in flat IP address will be at the same network. It's too large to manage practically. Now if we divide it into smaller network by extending network prefix from 16 bits to, say 24 bits, that's using its third byte to subnet this class B network. Now it has a subnet mask 255.255.255.0, in which each bit of the first three bytes is 1. It's now clear that the first two bytes is used to identify the class B network, the third byte is used to identify the subnet within this class B network and, of course, the last byte is the host number.

Not all IP address is available in the sub-netted network. Two special addresses are reserved. They are the addresses with all zero's and all one's host number. For example, an IP address 128.1.2.128, what IP address reserved will be looked like? All 0s mean the network itself, and all 1s mean IP broadcast.



In this diagram, you can see the subnet mask with 25-bit long, 255.255.255.128, contains 126 members in the sub-netted network. Another is that the length of network prefix equals the number of the bit with 1s in that subnet mask. With this, you can easily count the number of IP addresses matched. The following table shows the result.

Prefix Length	No. of IP matched	No. of Addressable IP
/32	1	-
/31	2	-
/30	4	2
/29	8	6
/28	16	14
/27	32	30
/26	64	62
/25	128	126
/24	256	254
/23	512	510
/22	1024	1022
/21	2048	2046
/20	4096	4094
/19	8192	8190
/18	16384	16382
/17	32768	32766
/16	65536	65534

Table 2-4

According to the scheme above, a subnet mask 255.255.255.0 will partition a network with the class C. It means there will have a maximum of 254 effective nodes existed in this sub-netted network and is considered a physical network in an autonomous network. So it owns a network IP address which may looks like 168.1.2.0.

With the subnet mask, a bigger network can be cut into small pieces of network. If we want to have more than two independent networks in a worknet, a partition to the network must be performed. In this case, subnet mask must be applied.

For different network applications, the subnet mask may look like 255.255.255.240. This means it is a small network accommodating a maximum of 15 nodes in the network.

Default gateway:

For the routed packet, if the destination is not in the routing table, all the traffic is put into the device with the designated IP address, known as default router. Basically, it is a routing policy. The gateway setting is used for Trap Events Host only in the switch.

For assigning an IP address to the switch, you just have to check what the IP address of the network will be connected with the switch. Use the same network address and append your host address to it.

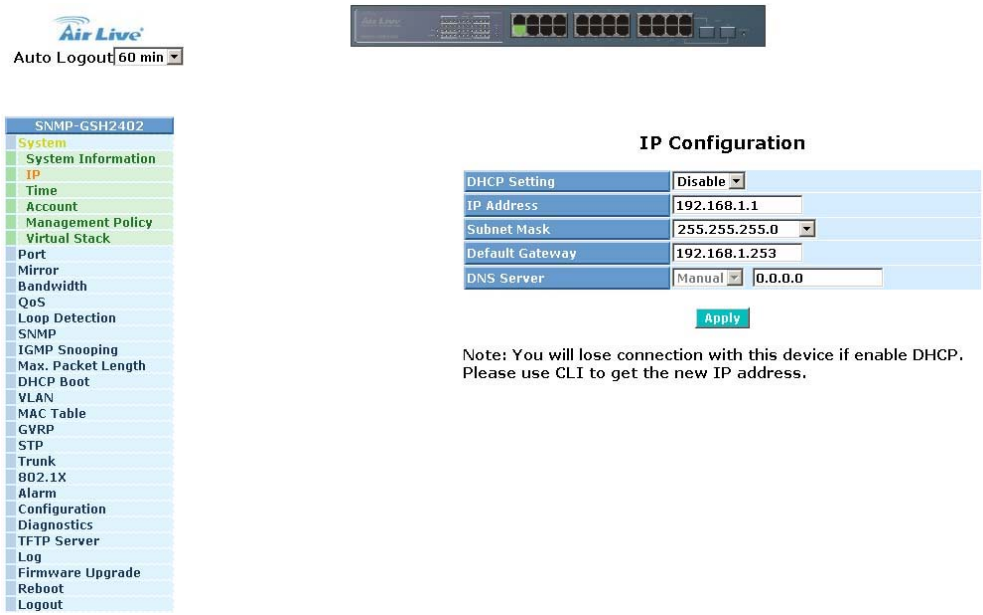


Fig. 2-12

First, IP Address: as shown in the Fig. 2-12, enter “192.168.1.1”, for instance. For sure, an IP address such as 192.168.1.x must be set on your PC.

Second, Subnet Mask: as shown in the Fig. 2-12, enter “255.255.255.0”. Any subnet mask such as 255.255.255.x is allowable in this case.

DNS:

The Domain Name Server translates human readable machine name to IP address. Every machine on the Internet has a unique IP address. A server generally has a static IP address. To connect to a server, the client needs to know the IP of the server. However, user generally uses the name to connect to the server. Thus, the switch DNS client program (such as a browser) will ask the DNS to resolve the IP address of the named server.

2-2. Typical Applications

The SNMP-GSH2416 SNMP Managed Gigabit Switch L2 Managed Switch implements 8 Gigabit Ethernet TP ports with auto MDIX and 16 slots for the removable module supporting comprehensive fiber types of connection, including LC and BiDi-LC SFP modules. For more details on the specification of the switch, please refer to Appendix A.

The switch is suitable for the following application.

— Central Site/Remote site application is used in carrier or ISP (See Fig. 2-13)

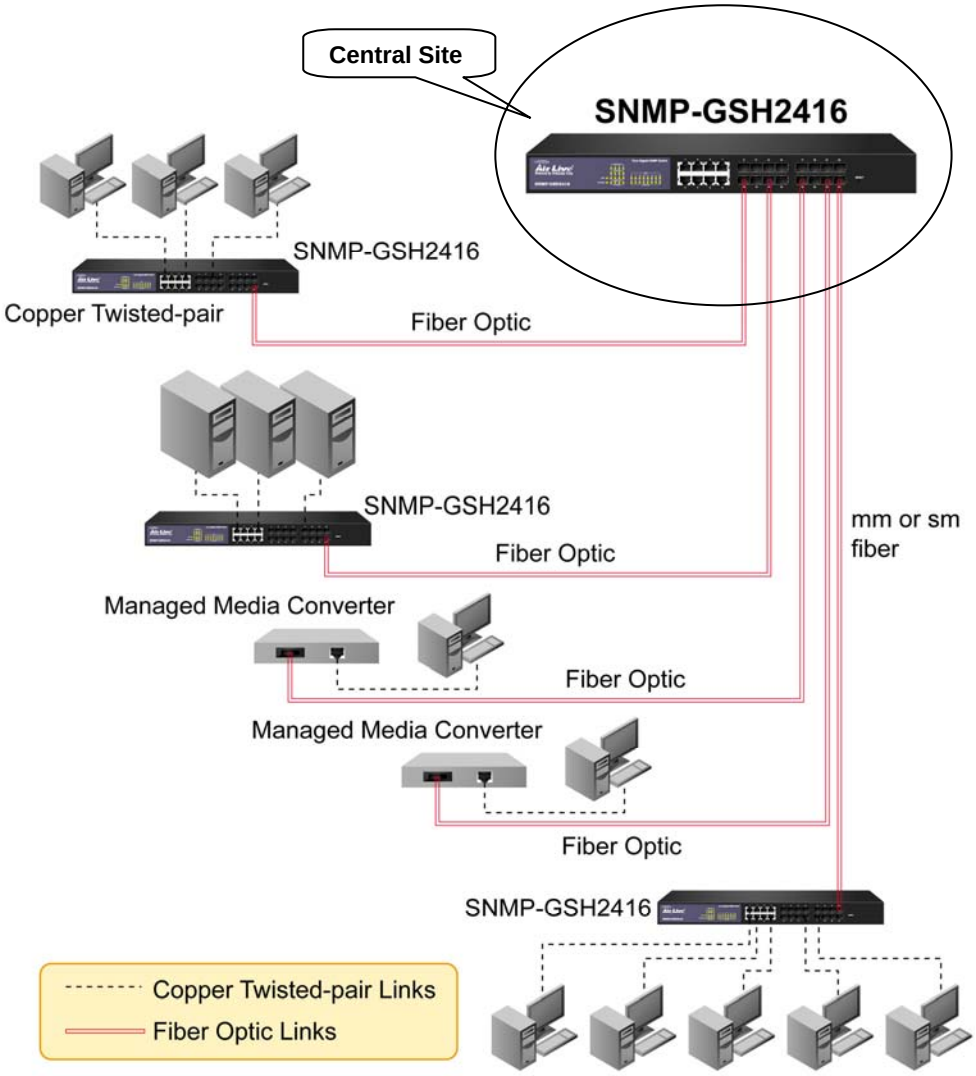


Fig. 2-13 Network Connection between Remote Site and Central Site

Fig. 2-13 is a system wide basic reference connection diagram. This diagram demonstrates how the switch connects with other network devices and hosts.

3. Operation of Web-based Management

This chapter instructs you how to configure and manage the switch through the web user interface it supports, to access and manage the 8-Port 10/100/1000Mbps TP and 16-Port Gigabit SFP Fiber management Ethernet switch. With this facility, you can easily access and monitor through any one port of the switch all the status of the switch, including MIBs status, each port activity, Spanning tree status, port aggregation status, multicast traffic, VLAN and priority status, even illegal access record and so on.

The default values of the managed switch are listed in the table below:

IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.254
Username	admin
Password	admin

Table 3-1

After the managed switch has been finished configuration in the CLI via the switch's serial interface, you can browse it. For instance, type http://192.168.1.1 in the address row in a browser, it will show the following screen (see Fig.3-1) and ask you inputting username and password in order to login and access authentication. The default username and password are both "admin". For the first time to use, please enter the default username and password, then click the **<Login>** button. The login process now is completed.

Just click the link of "Forget Password" in WebUI (See Fig. 3-1) or input "Ctrl+Z" in CLI's login screen (See Fig. 4-1~4-2) in case the user forgets the manager's password. Then, the system will display a serial No. for the user. Write down this serial No. and contact your vendor, the vendor will give you a temporary password. Use this new password as ID and Password, and it will allow the user to login the system with manager authority temporarily. Due to the limit of this new password, the user only can login the system one time, therefore, please modify your password immediately after you login in the system successfully.

In this login menu, you have to input the complete username and password respectively, the switch will not give you a shortcut to username automatically. This looks inconvenient, but safer.

In the switch, it supports a simple user management function allowing only one administrator to configure the system at the same time. If there are two or more users using administrator's identity, the switch will allow the only one who logins first to configure the system. The rest of users, even with administrator's identity, can only monitor the system. For those who have no administrator's identity, can only monitor the system. There are only a maximum of three users able to login simultaneously in the switch.

To optimize the display effect, we recommend you use Microsoft IE 6.0 above, Netscape V7.1 above or FireFox V1.00 above and have the resolution 1024x768. The switch supported neutral web browser interface.

In Fig. 3-2, for example, left section is the whole function tree with web user interface and we will travel it through this chapter.

Fig. 3-1

3-1. Web Management Home Overview

After you login, the switch shows you the system information as Fig. 3-2. This page is default and tells you the basic information of the system, including “Model Name”, “System Description”, “Location”, “Contact”, “Device Name”, “System Up Time”, “Current Time”, “BIOS Version”, “Firmware Version”, “Hardware-Mechanical Version”, “Serial Number”, “Host IP Address”, “Host Mac Address”, “Device Port”, “RAM Size” and “Flash Size”. With this information, you will know the software version used, MAC address, serial number, how many ports good and so on. This is helpful while malfunctioning.

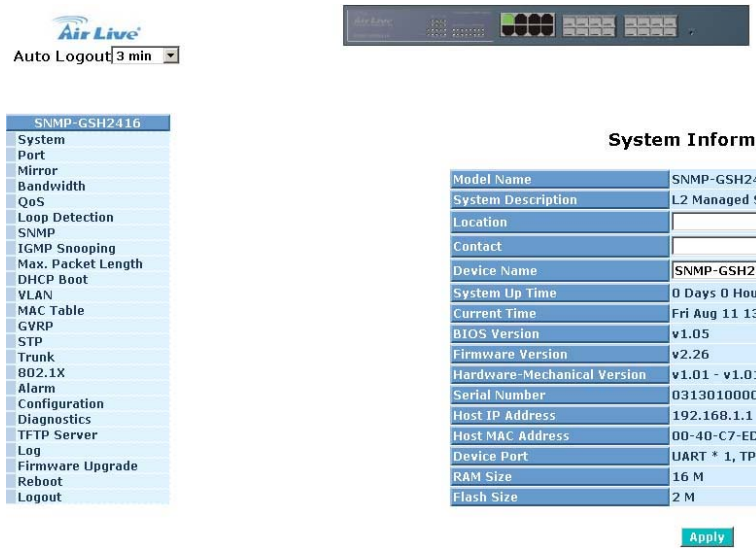


Fig. 3-2

- **The Information of Page Layout**

— On the top side, it shows the front panel of the switch. In the front panel, the linked ports will display green; as to the ports, which are link off, they will be dark. For the optional modules, the slot will show only a cover plate if no module exists and will show a module if a module is present. The image of module depends on the one you inserted. The same, if disconnected, the port will show just dark, if linked, green.

In this device, there are clicking functions on the panel provided for the information of the ports. These are very convenient functions for browsing the information of a single port. When clicking the port on the front panel, an information window for the port will be pop out. (See Fig. 3-3)

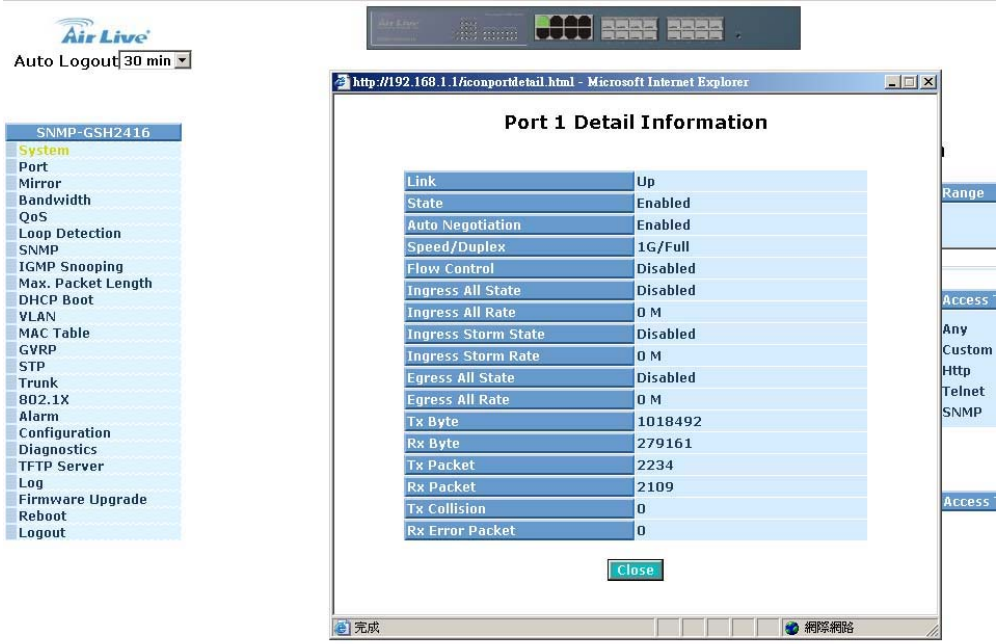


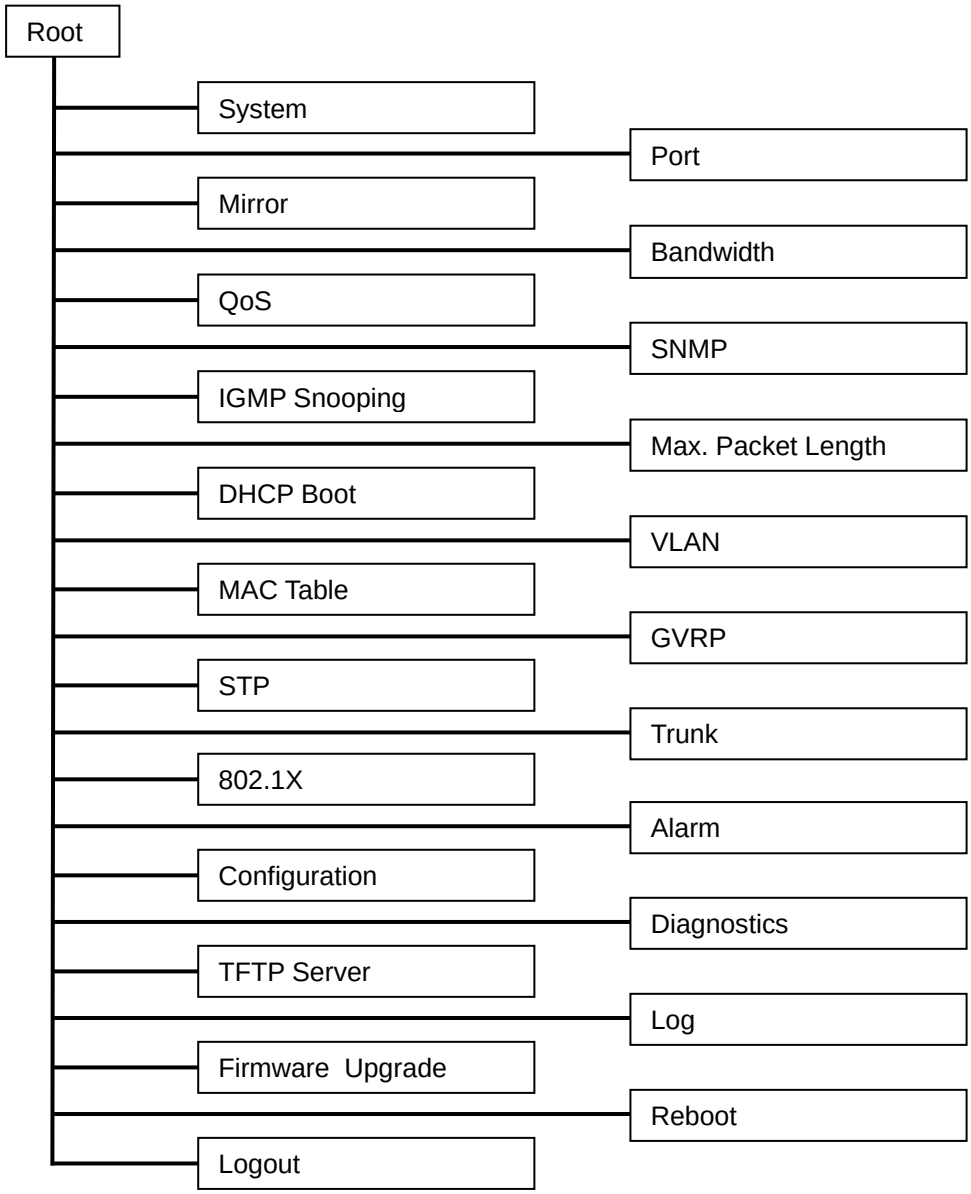
Fig. 3-3 port detail information

In Fig. 3-3, it shows the basic information of the clicked port. With this, you'll see the information about the port status, traffic status and bandwidth rating for egress and ingress respectively.

— On the left-top corner, there is a pull-down list for Auto Logout. For the sake of security, we provide auto-logout function to protect you from illegal user as you are leaving. If you do not choose any selection in Auto Logout list, it means you turn on the Auto Logout function and the system will be logged out automatically when no action on the device 3 minutes later. If OFF is chosen, the screen will keep as it is. Default is ON.

— On the left side, the main menu tree for web is listed in the page. They are hierarchical menu. Open the function folder, a sub-menu will be shown. The functions of each folder are described in its corresponded section respectively. When clicking it, the function is performed. The following list is the full function

tree for web user interface.



3-1-1. System Information

Function name:

System Information

Function description:

Show the basic system information.

Parameter description:

Model name:

The model name of this device.

System description:

As it is, this tells what this device is. Here, it is “L2 Managed Switch”.

Location:

Basically, it is the location where this switch is put. User-defined.

Contact:

For easily managing and maintaining device, you may write down the contact person and phone here for getting help soon. You can configure this parameter through the device’s user interface or SNMP.

Device name:

The name of the switch. User-defined. Default is SNMP-GSH2416.

System up time:

The time accumulated since this switch is powered up. Its format is day, hour, minute, second.

Current time:

Show the system time of the switch. Its format: day of week, month, day, hours : minutes : seconds, year. For instance, Wed, Apr. 23, 12:10:10, 2004.

BIOS version:

The version of the BIOS in this switch.

Firmware version:

The firmware version in this switch.

Hardware-Mechanical version:

The version of Hardware and Mechanical. The figure before the hyphen is the version of electronic hardware; the one after the hyphen is the version of mechanical.

Serial number:

The serial number is assigned by the manufacturer.

Host IP address:

The IP address of the switch.

Host MAC address:

It is the Ethernet MAC address of the management agent in this switch.

Device Port:

Show all types and numbers of the port in the switch.

RAM size:

The size of the DRAM in this switch.

Flash size:

The size of the flash memory in this switch.

3-1-2. IP Configuration

IP configuration is one of the most important configurations in the switch. Without the proper setting, network manager will not be able to manage or view the device. The switch supports both manual IP address setting and automatic IP address setting via DHCP server. When IP address is changed, you must reboot the switch to have the setting taken effect and use the new IP to browse for web management and CLI management.

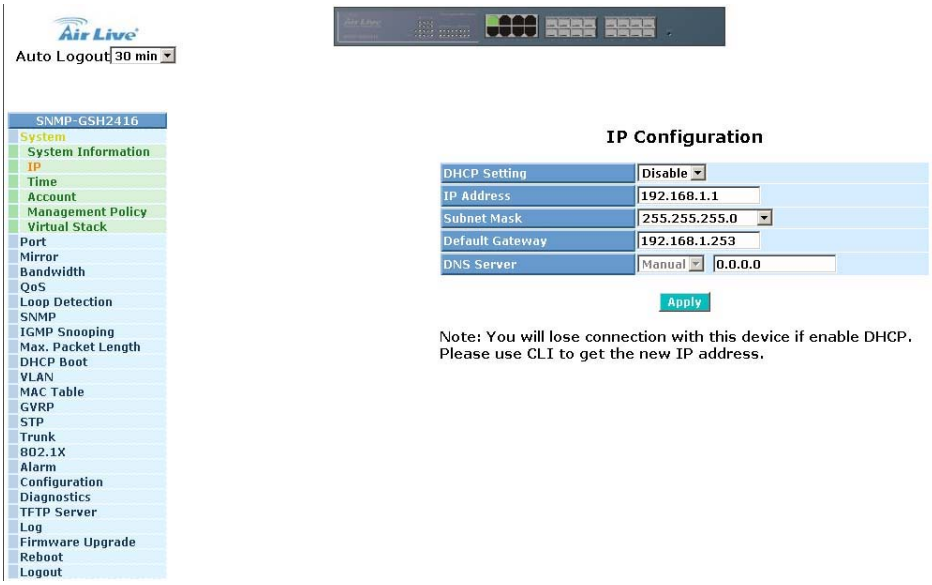


Fig. 3-4 IP Address Configuration

Function name:

IP Configuration

Function description:

Set IP address, subnet mask, default gateway and DNS for the switch.

Parameter description:

DHCP Setting:

DHCP is the abbreviation of Dynamic Host Configuration Protocol. Here DHCP means a switch to turn ON or OFF the function.

The switch supports DHCP client used to get an IP address automatically if you set this function “Enable”. When enabled, the switch will issue the request to the DHCP server resided in the network to get an IP address. If DHCP server is down or does not exist, the switch will issue the request and show IP address is under requesting, until the DHCP server is up. Before getting an IP address from DHCP server, the device will not continue booting procedures. If set this field “Disable”, you’ll have to input IP address manually. For more details about IP address and DHCP, please see the Section 2-1-5 “IP Address Assignment” in this manual.

Default: Disable

IP address:

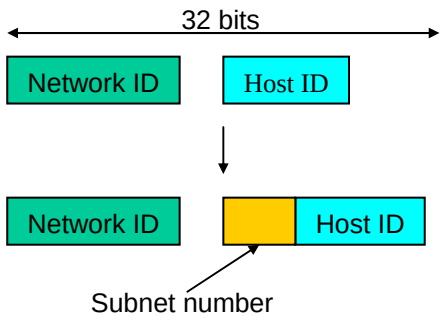
Users can configure the IP settings and fill in new values if users set the DHCP function “Disable”. Then, click **<Apply>** button to update.

When DHCP is disabled, Default: 192.168.1.1

If DHCP is enabled, this field is filled by DHCP server and will not allow user manually set it any more.

Subnet mask:

Subnet mask is made for the purpose to get more network address because any IP device in a network must own its IP address, composed of Network address and Host address, otherwise can’t communicate with other devices each other. But unfortunately, the network classes A, B, and C are all too large to fit for almost all networks, hence, subnet mask is introduced to solve this problem. Subnet mask uses some bits from host address and makes an IP address looked Network address, Subnet mask number and host address. It is shown in the following figure. This reduces the total IP number of a network able to support, by the amount of 2 power of the bit number of subnet number (2^(bit number of subnet number)).



Subnet mask is used to set the subnet mask value, which should be the same value as that of the other devices resided in the same network it attaches.

For more information, please also see the Section 2-1-5 “IP Address Assignment” in this manual.

Default: 255.255.255.0

Default gateway:

Set an IP address for a gateway to handle those packets that do not meet the routing rules predefined in the device. If a packet does not meet the criteria for other pre-defined path, it must be forwarded to a default router on a default path. This means any packet with undefined IP address in the routing table will be sent to this device unconditionally.

Default: 192.168.1.254

DNS:

It is Domain Name Server used to serve the translation between IP address and name address.

The switch supports DNS client function to re-route the mnemonic name address to DNS server to get its associated IP address for accessing Internet. User can specify a DNS IP address for the switch. With this, the switch can translate a mnemonic name address into an IP address.

There are two ways to specify the IP address of DNS. One is fixed mode, which manually specifies its IP address, the other is dynamic mode, which is assigned by DHCP server while DHCP is enabled. DNS can help you easily remember the mnemonic address name with the meaningful words in it. Default is no assignment of DNS address.

Default: 0.0.0.0

3-1-3. Time Configuration

The switch provides manual and automatic ways to set the system time via NTP. Manual setting is simple and you just input “Year”, “Month”, “Day”, “Hour”, “Minute” and “Second” within the valid value range indicated in each item. If you input an invalid value, for example, 61 in minute, the switch will clamp the figure to 59.

NTP is a well-known protocol used to synchronize the clock of the switch system time over a network. NTP, an internet draft standard formalized in RFC 1305, has been adopted on the system is version 3 protocol. The switch provides four built-in NTP server IP addresses resided in the Internet and an user-defined NTP server IP address. The time zone is Greenwich-centered which uses the expression form of GMT+/- xx hours.

Function name:

Time

Function description:

Set the system time by manual input or set it by syncing from Time servers. The function also supports daylight saving for different area’s time adjustment.

Parameter description:

Current Time:

Show the current time of the system.

Manual:

This is the function to adjust the time manually. Filling the valid figures in the fields of Year, Month, Day, Hour, Minute and Second respectively and press **<Apply>** button, time is adjusted. The valid figures for the parameter Year, Month, Day, Hour, Minute and Second are >=2000, 1-12, 1-31, 0-23, 0-59 and 0-59 respectively. Input the wrong figure and press **<Apply>** button, the device will reject the time adjustment request. There is no time zone setting in Manual mode.

Default: Year = 2000, Month = 1, Day = 1
Hour = 0, Minute = 0, Second = 0

NTP:

NTP is Network Time Protocol and is used to sync the network time based Greenwich Mean Time (GMT). If use the NTP mode and select a built-in NTP time server or manually specify an user-defined NTP server as well as Time Zone, the switch will sync the time in a short after pressing **<Apply>** button. Though it synchronizes the time automatically, NTP does not update the time periodically without user's processing.

Time Zone is an offset time off GMT. You have to select the time zone first and then perform time sync via NTP because the switch will combine this time zone offset and updated NTP time to come out the local time, otherwise, you will not able to get the correct time. The switch supports configurable time zone from –12 to +13 step 1 hour.

Default Time zone: +8 Hrs.

Daylight Saving:

Daylight saving is adopted in some countries. If set, it will adjust the time lag or in advance in unit of hours, according to the starting date and the ending date. For example, if you set the day light saving to be 1 hour. When the time passes over the starting time, the system time will be increased one hour after one minute at the time since it passed over. And when the time passes over the ending time, the system time will be decreased one hour after one minute at the time since it passed over.

The switch supports valid configurable day light saving time is –5 ~ +5 step one hour. The zero for this parameter means it need not have to adjust current time, equivalent to in-act daylight saving. You don't have to set the starting/ending date as well. If you set daylight saving to be non-zero, you have to set the starting/ending date as well; otherwise, the daylight saving function will not be activated.

Default for Daylight Saving: 0.

The following parameters are configurable for the function Daylight Saving and described in detail.

Day Light Saving Start :

This is used to set when to start performing the day light saving time.

Mth:

Range is 1 ~ 12.

Default: 1

Day:

Range is 1 ~ 31.

Default: 1

Hour:

Range is 0 ~ 23.

Default: 0

Day Light Saving End :

This is used to set when to stop performing the daylight saving time.

Mth:

Range is 1 ~ 12.

Default: 1

Day:

Range is 1 ~ 31.

Default: 1

Hour:

Range is 0 ~ 23.

Default: 0

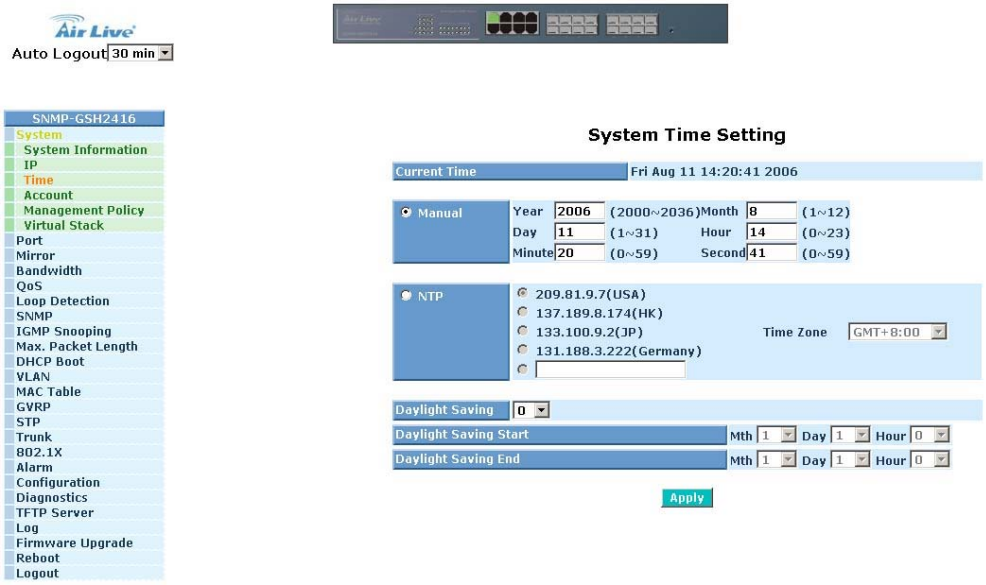


Fig. 3-5

3-1-4. Account Configuration

In this function, only administrator can create, modify or delete the username and password. Administrator can modify other guest identities' password without confirming the password but it is necessary to modify the administrator-equivalent identity. Guest-equivalent identity can modify his password only. Please note that you must confirm administrator/guest identity in the field of Authorization in advance before configuring the username and password. Only one administrator is allowed to exist and unable to be deleted. In addition, up to 4 guest accounts can be created.

The default setting for user account is:

Username : admin

Password : admin

The default setting for guest user account is:

Username : guest

Password : guest

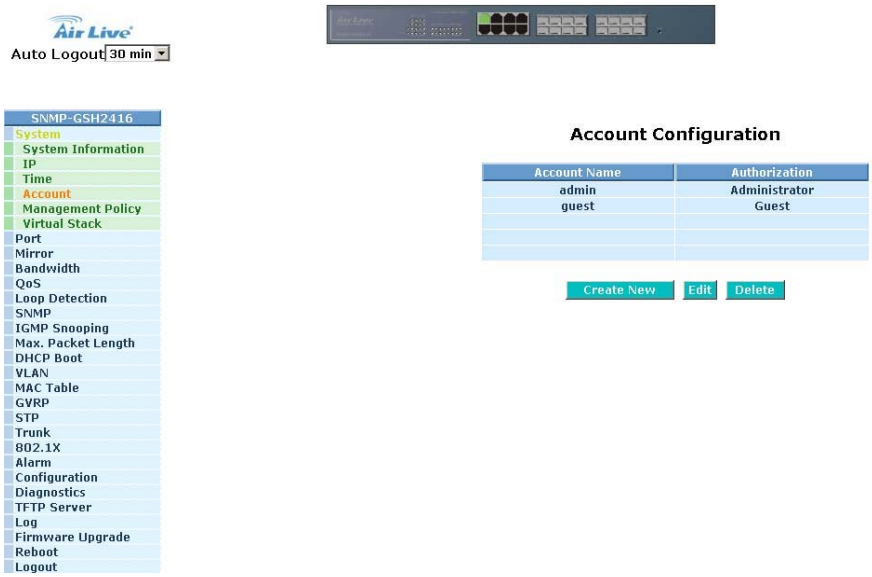


Fig. 3-6

3-1-5. Management Policy

Through the management security configuration, the manager can do the strict setup to control the switch and limit the user to access this switch.

The following rules are offered for the manager to manage the switch:

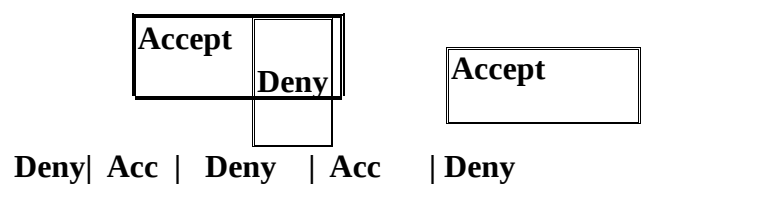
Rule 1) : When no lists exists, then it will accept all connections.

Rule 2) : When only "accept lists" exist, then it will deny all connections, excluding the connection inside of the accepting range.

Rule 3) : When only "deny lists" exist, then it will accept all connections, excluding the connection inside of the denying range.

Rule 4) : When both "accept and deny" lists exist, then it will deny all connections, excluding the connection inside of the accepting range.

Rule 5) : When both "accept and deny" lists exist, then it will deny all connections, excluding the connection inside of the accepting range and NOT inside of the denying range at the same time.



Function name:

Management Security Configuration

Function description:

The switch offers Management Security Configuration function. With this function, the manager can easily control the mode that the user connects to the switch. According to the mode, users can be classified into two types: Those who are able to connect to the switch (Accept) and those who are unable to connect to the switch (Deny). Some restrictions also can be placed on the mode that the user connect to the switch, for example, we can decide that which VLAN VID is able to be accepted or denied by the switch, the IP range of the user could be accepted or denied by the switch, the port that the user is allowed or not allowed to connect with the switch, or the way of controlling and connecting to the switch via Http, Telnet or SNMP.

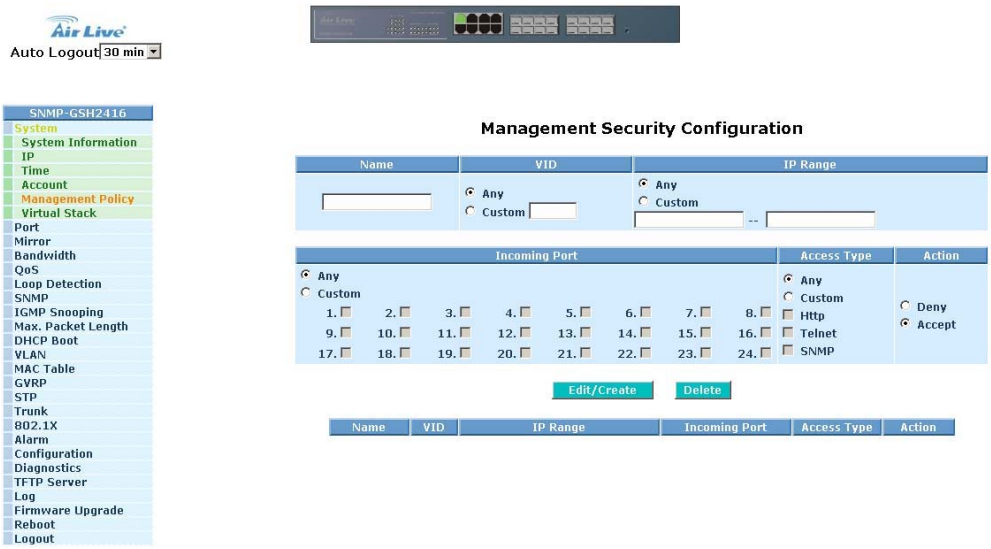


Fig. 3-7

Parameter description:

Name:

A name is composed of any letter (A-Z, a-z) and digit (0-9) with maximal 8 characters.

VID:

The switch supports two kinds of options for managed valid VLAN VID, including “Any” and “Custom”. Default is “Any”. When you choose “Custom”, you can fill in VID number. The valid VID range is 1~4094.

IP Range:

The switch supports two kinds of options for managed valid IP Range, including “Any” and “Custom”. Default is “Any”. In case that” Custom” had been chosen, you can assigned effective IP range. The valid range is 0.0.0.0~255.255.255.255.

Incoming Port:

The switch supports two kinds of options for managed valid Port Range, including “Any” and “Custom”. Default is “Any”. You can select the ports that you would like them to be worked and restricted in the management security configuration if ”Custom” had been chosen.

Access Type:

The switch supports two kinds of options for managed valid Access Type, including “Any” and “Custom”. Default is “Any”. “Http”, “Telnet” and “SNMP” are three ways for the access and managing the switch in case that” Custom” had been chosen.

Action:

The switch supports two kinds of options for managed valid Action Type, including “Deny” and “Accept”. Default is “Deny”. When you choose “Deny” action, you will be restricted and refused to manage the switch due to the “Access Type” you choose. However, while you select “Accept” action, you will have the authority to manage the switch.

Edit/Create:

A new entry of Management Security Configuration can be created after the parameters as mentioned above had been setup and then press **<Edit/Create>** button. Of course, the existed entry also can be modified by pressing this button.

Delete:

Remove the existed entry of Management Security Configuration from the management security table.

3-1-6. Virtual Stack

Function name:

Virtual Stack

Function description:

Virtual Stack Management(VSM) is the group management function. Through the proper configuration of this function, switches in the same LAN will be grouped automatically. And among these switch, one switch will be a master machine, and the others in this group will become the slave devices.

VSM offers a simple centralized management function. It is not necessary to remember the address of all devices, manager is capable of managing the network with knowing the address of the Master machine. Instead of SNMP or Telnet UI, VSM is only available in Web UI. While one switch become the Master, two rows of buttons for group device will appear on the top of its Web UI. By pressing these buttons, user will be allowed to connect the Web UI of the devices of the group in the same window without the login of these device.

The most top-left button is only for Master device(See Fig.3-9). The background color of the button you press will be changed to represent that the device is under your management.

Note: It will remove the grouping temporarily in case that you login the switch via the console.

The device of the group will be shown as station address (the last number of IP Address) + device name on the button (e.g. 196_SNMP-GSH2416), otherwise it will show ” ---- “ if no corresponding device exists.

Once the devices join the group successfully, then they are merely able to be managed via Master device, and user will fail to manage them via telnet/console/web individually.

Up to 16 devices can be grouped for VSM, however, only one Master is allowed to exist in each group. For Master redundancy, user may configure more than two devices as Master device, however, the Master device with the smaller MAC value will be the Master one. All of these 16 devices can become Master device and back up with each other .

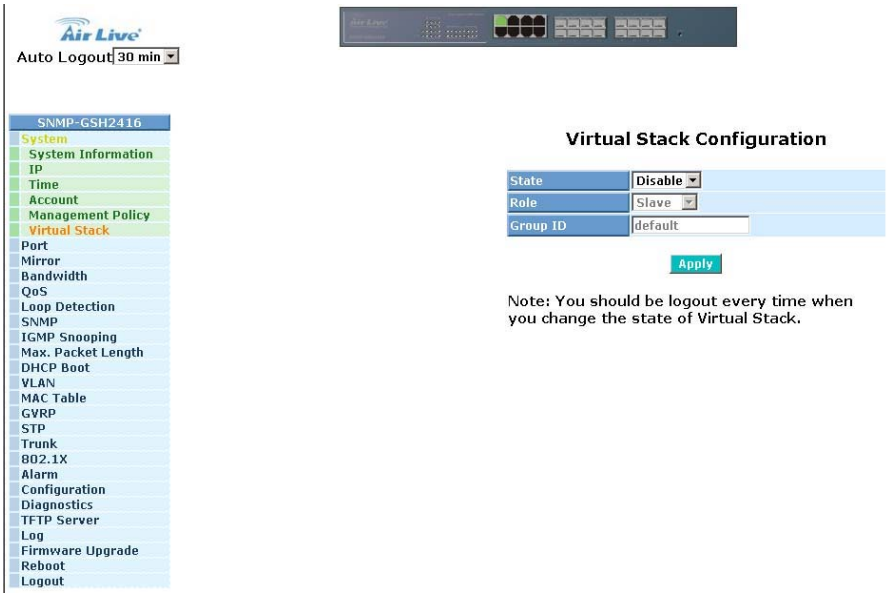


Fig. 3-8

Parameter description:

State:

It is used for the activation or de-activation of VSM. Default is Enable.

Role:

The role that the switch would like to play in virtual stack. Two types of roles, including master and slave are offered for option. Default is Master.

Group ID:

It is the group identifier (GID) which signs for VSM. Valid letters are A-Z, a-z, 0-9, " - " and "_" characters. The maximal length is 15 characters.

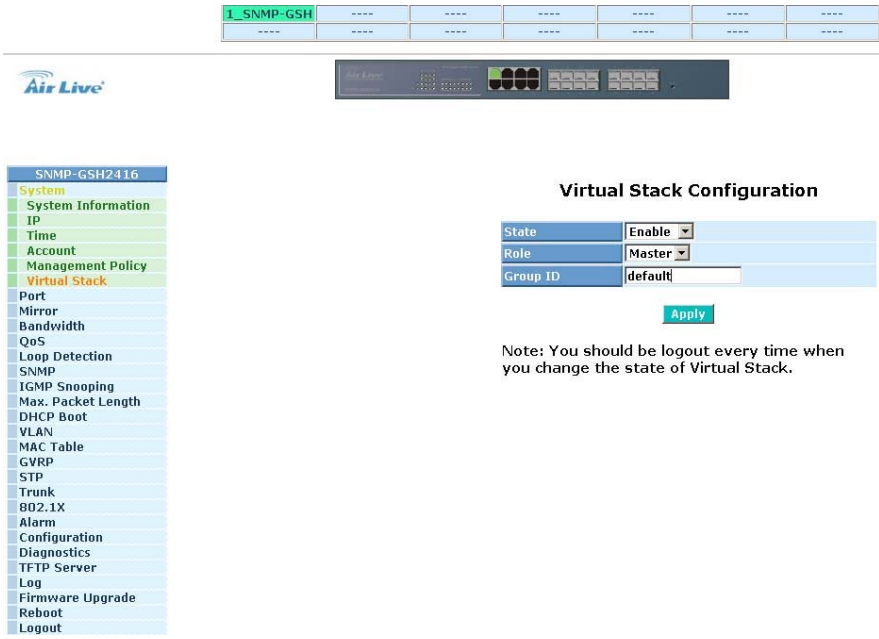
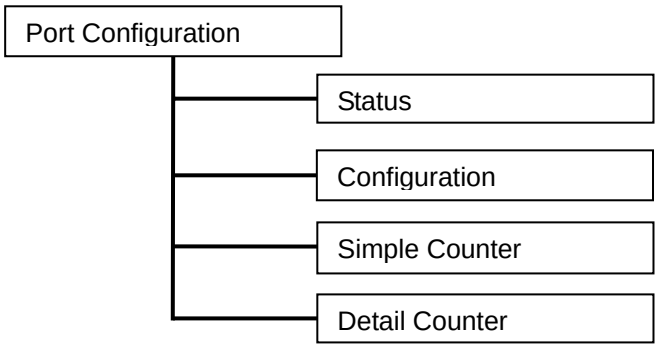

1_SNMP-GSH
SNMP-GSH2416
System
System Information
IP
Time
Account
Management Policy
Virtual Stack
Port
Mirror
Bandwidth
QoS
Loop Detection
SNMP
IGMP Snooping
Max. Packet Length
DHCP Boot
VLAN
MAC Table
GVRP
STP
Trunk
802.1X
Alarm
Configuration
Diagnostics
TFTP Server
Log
Firmware Upgrade
Reboot
Logout
Virtual Stack Configuration
State
Enable
Role
Master
Group ID
default
Apply
Note: You should be logout every time when you change the state of Virtual Stack.

Fig. 3-9

3-2. Port Configuration

Four functions, including Port Status, Port Configuration, Simple Counter and Detail Counter are contained in this function folder for port monitor and management. Each of them will be described in detail orderly in the following sections.



3-2-1.Port Status

The function Port Status gathers the information of all ports' current status and reports it by the order of port number, link status, port state, Auto-Negotiation status, speed/duplex and flow control. An extra media type information for the module port 9 to 24 is also offered (See Fig. 3-11).

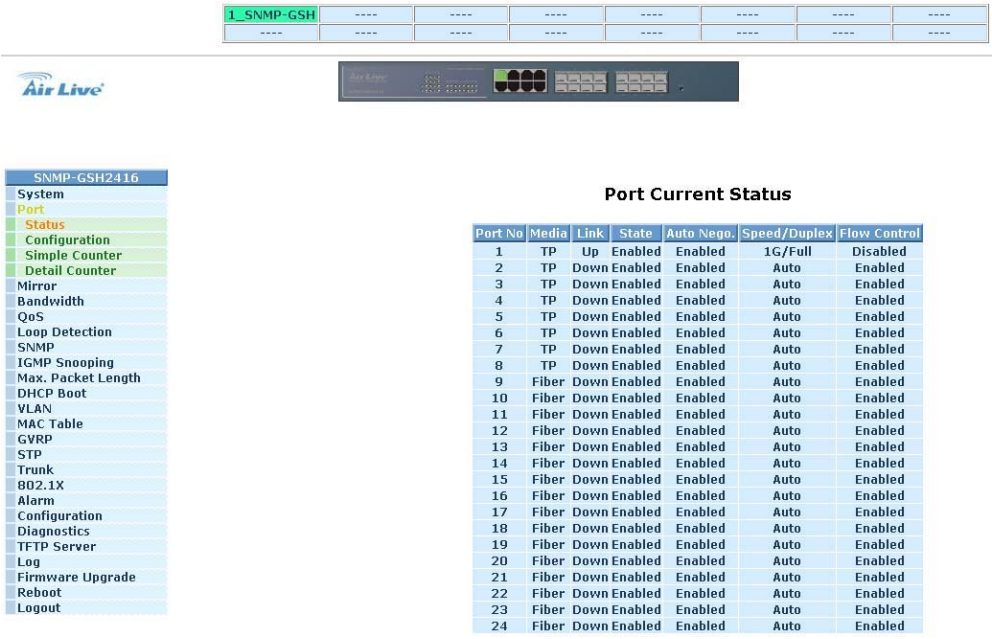

1_SNMP-GSH
SNMP-GSH2416
System
Port
Status
Configuration
Simple Counter
Detail Counter
Mirror
Bandwidth
QoS
Loop Detection
SNMP
IGMP Snooping
Max. Packet Length
DHCP Boot
VLAN
MAC Table
GVRP
STP
Trunk
802.1X
Alarm
Configuration
Diagnostics
TFTP Server
Log
Firmware Upgrade
Reboot
Logout
Port Current Status
Port No Media Link State Auto Nego. Speed/Duplex Flow Control
1 TP Up Enabled Enabled 1G/Full Disabled
2 TP Down Enabled Enabled Auto Enabled
3 TP Down Enabled Enabled Auto Enabled
4 TP Down Enabled Enabled Auto Enabled
5 TP Down Enabled Enabled Auto Enabled
6 TP Down Enabled Enabled Auto Enabled
7 TP Down Enabled Enabled Auto Enabled
8 TP Down Enabled Enabled Auto Enabled
9 Fiber Down Enabled Enabled Auto Enabled
10 Fiber Down Enabled Enabled Auto Enabled
11 Fiber Down Enabled Enabled Auto Enabled
12 Fiber Down Enabled Enabled Auto Enabled
13 Fiber Down Enabled Enabled Auto Enabled
14 Fiber Down Enabled Enabled Auto Enabled
15 Fiber Down Enabled Enabled Auto Enabled
16 Fiber Down Enabled Enabled Auto Enabled
17 Fiber Down Enabled Enabled Auto Enabled
18 Fiber Down Enabled Enabled Auto Enabled
19 Fiber Down Enabled Enabled Auto Enabled
20 Fiber Down Enabled Enabled Auto Enabled
21 Fiber Down Enabled Enabled Auto Enabled
22 Fiber Down Enabled Enabled Auto Enabled
23 Fiber Down Enabled Enabled Auto Enabled
24 Fiber Down Enabled Enabled Auto Enabled

Fig. 3-10

Function name:

Port Status

Function Description:

Report the latest updated status of all ports in this switch. When any one of the ports in the switch changes its parameter displayed in the page, it will be automatically refreshed the port current status about every 5 seconds.

Parameter Description:

Port No:

Display the port number. The number is 1 – 24.

Media:

Show the media type adopted in all ports. The Port 9 to Port 24 are SFP fiber modules, which support fiber media with Gigabit Ethernet (1000Mbps) only. They may have different media types and speed. Especially, fiber port has comprehensive types of connector, distance, fiber mode and so on. The switch describes the module ports with the following page.

Link:

Show that if the link on the port is active or not. If the link is connected to a working-well device, the Link will show the link “Up”; otherwise, it will show “Down”. This is determined by the hardware on both devices of the connection.

No default value.

State:

Show that the communication function of the port is “Enabled” or “Disabled”. When it is enabled, traffic can be transmitted and received via this port. When it is disabled, no traffic can be transferred through this port. Port State is configured by user.

Default: Enabled.

Auto Negotiation:

Show the exchange mode of Ethernet MAC. There are two modes supported in the switch. They are auto-negotiation mode “Enabled” and forced mode “Disabled”. When in “Enabled” mode, this function will automatically negotiate by hardware itself and exchange each other the capability of speed and duplex mode with other site which is linked, and comes out the best communication way. When in “Disabled” mode, both parties must have the same setting of speed and duplex, otherwise, both of them will not be linked. In this case, the link result is “Down”.

Default: Enabled

Speed / Duplex Mode:

Display the speed and duplex of all port. There are three speeds 10Mbps, 100Mbps and 1000Mbps supported for TP media, and the duplex supported is half duplex and full duplex. If the media is 1Gbps fiber, it is 1000Mbps supported only. The status of speed/duplex mode is determined by 1) the negotiation of both local port and link partner in “Auto Speed” mode or 2) user setting in “Force” mode. The local port has to be preset its capability.

Default: None, depends on the result of the negotiation.

Flow Control:

Show each port’s flow control status.

There are two types of flow control in Ethernet, Backpressure for half-duplex operation and Pause flow control (IEEE802.3x) for full-duplex operation. The switch supports both of them.

Default: Disabled

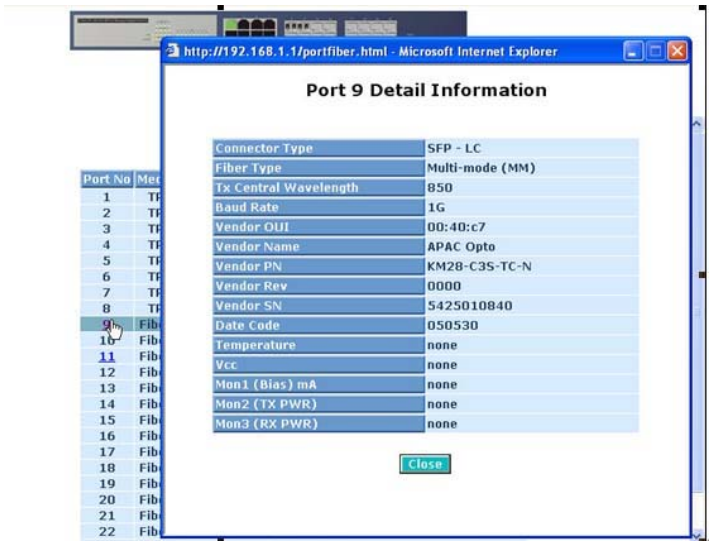


Fig. 3-11

Parameter description of Port 9~24:

Connector Type:

Display the connector type, for instance, UTP, SC, ST, LC and so on.

Fiber Type:

Display the fiber mode, for instance, Multi-Mode, Single-Mode.

Tx Central Wavelength:

Display the fiber optical transmitting central wavelength, for instance, 850nm, 1310nm, 1550nm and so on.

Baud Rate:

Display the maximum baud rate of the fiber module supported, for instance, 10M, 100M, 1G and so on.

Vendor OUI:

Display the Manufacturer's OUI code which is assigned by IEEE.

Vendor Name:

Display the company name of the module manufacturer.

Vendor P/N:

Display the product name of the naming by module manufacturer.

Vendor Rev (Revision):

Display the module revision.

Vendor SN (Serial Number):

Show the serial number assigned by the manufacturer.

Date Code:

Show the date this SFP module was made.

Temperature:

Show the current temperature of SFP module.

Vcc:

Show the working DC voltage of SFP module.

Mon1(Bias) mA:

Show the Bias current of SFP module.

Mon2(TX PWR):

Show the transmit power of SFP module.

Mon3(RX PWR):

Show the receiver power of SFP module.

3-2-2. Port Configuration

Port Configuration is applied to change the setting of each port. In this configuration function, you can set/reset the following functions. All of them are described in detail below.

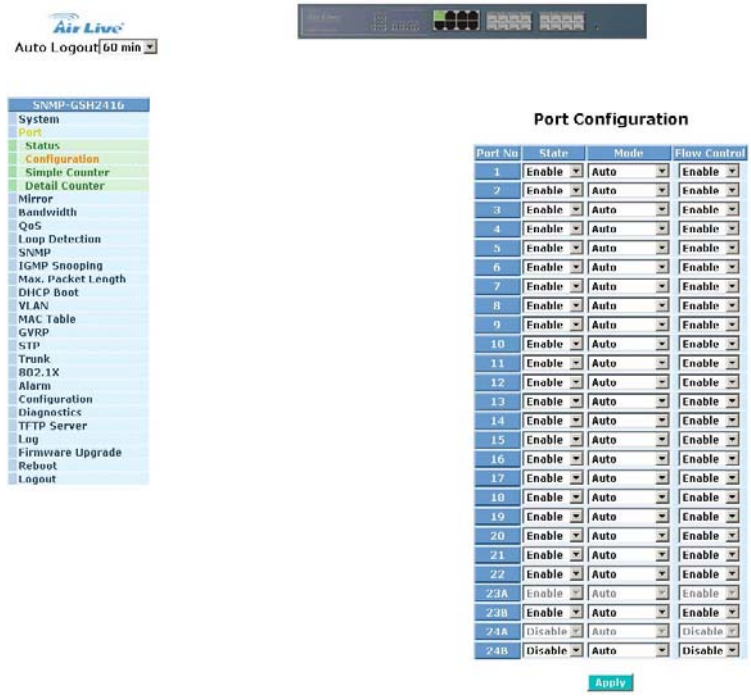


Fig. 3-12

Function name:

Port Configuration

Function description:

It is used to set each port's operation mode. The switch supports 3 parameters for each port. They are state, mode and flow control.

Parameter description:

State:

Set the communication capability of the port is Enabled or Disabled. When enabled, traffic can be transmitted and received via this port. When disabled, the port is blocked and no traffic can be transferred through this port. Port State is configurable by the user. There are only two states "Enable" and "Disable" able to choose. If you set a port's state "Disable", then that port is prohibited to pass any traffic, even it looks Link up.

Default: Enable.

Mode:

Set the speed and duplex of the port. In speed, if the media is 1Gbps fiber, it is always 1000Mbps and the duplex is full only. If the media is TP, the Speed/Duplex is comprised of the combination of speed mode, 10/100/1000Mbps, and duplex mode, full duplex and half duplex. The following table summarized the function the media supports.

Media type	NWay	Speed	Duplex
1000M TP	ON/OFF	10/100/1000M	Full for all, Half for 10/100
1000M Fiber	ON/OFF	1000M	Full

In Auto-negotiation mode, no default value. In Forced mode, default value depends on your setting.

Flow Control:

There are two modes to choose in flow control, including Enable and Disable. If flow control is set Enable, both parties can send PAUSE frame to the transmitting device(s) if the receiving port is too busy to handle. When it is set Disable, there will be no flow control in the port. It drops the packet if too much to handle.

Default: Enable.

3-2-3. Simple Counter

The function of Simple Counter collects any information and provides the counting about the traffic of the port, no matter the packet is good or bad.

In the Fig. 3-13, the window can show all ports' counter information at the same time. Each data field has 20-digit long. If the counting is overflow, the counter will be reset and restart counting. The data is updated every time interval defined by the user. The valid range is 3 to 10 seconds. The Refresh Interval is used to set the update frequency. Default update time is 3 seconds.

Air Live
Auto Logout 60 min
SNMP-GSH2416
System
Port
Status
Configuration
Simple Counter
Detail Counter
Mirror
Bandwidth
QoS
Loop Detection
SNMP
IGMP Snooping
Max. Packet Length
DHCP Boot
VLAN
MAC Table
GVRP
STP
Trunk
802.1X
Alarm
Configuration
Diagnostics
TFTP Server
Log
Firmware Upgrade
Reboot
Logout
Simple Counter
Refresh Interval 3 sec
Reset
Time elapsed since last reset: 0 Days 1 Hours 10 Mins 0 Secs
Port No | Tx Byte | Rx Byte | Tx Packet | Rx Packet | Tx Collision | Rx Error Packet
1 | 4993159 | 1066989 | 10165 | 8361 | 0 | 0
2 | 0 | 0 | 0 | 0 | 0 | 0
3 | 0 | 0 | 0 | 0 | 0 | 0
4 | 0 | 0 | 0 | 0 | 0 | 0
5 | 0 | 0 | 0 | 0 | 0 | 0
6 | 0 | 0 | 0 | 0 | 0 | 0
7 | 0 | 0 | 0 | 0 | 0 | 0
8 | 0 | 0 | 0 | 0 | 0 | 0
9 | 0 | 0 | 0 | 0 | 0 | 0
10 | 0 | 0 | 0 | 0 | 0 | 0
11 | 0 | 0 | 0 | 0 | 0 | 0
12 | 0 | 0 | 0 | 0 | 0 | 0
13 | 0 | 0 | 0 | 0 | 0 | 0
14 | 0 | 0 | 0 | 0 | 0 | 0
15 | 0 | 0 | 0 | 0 | 0 | 0
16 | 0 | 0 | 0 | 0 | 0 | 0
17 | 0 | 0 | 0 | 0 | 0 | 0
18 | 0 | 0 | 0 | 0 | 0 | 0
19 | 0 | 0 | 0 | 0 | 0 | 0
20 | 0 | 0 | 0 | 0 | 0 | 0
21 | 0 | 0 | 0 | 0 | 0 | 0
22 | 0 | 0 | 0 | 0 | 0 | 0
23 | 0 | 0 | 0 | 0 | 0 | 0
24 | 0 | 0 | 0 | 0 | 0 | 0

Fig. 3-13

Function name:

Simple Counter

Function description:

Display the summary counting of each port's traffic, including Tx Byte, Rx Byte, Tx Packet, Rx Packet, Tx Collision and Rx Error Packet.

Parameters description:

Tx Byte:

Total transmitted bytes.

Rx Byte:

Total received bytes.

Tx Packet:

The counting number of the packet transmitted.

Rx Packet:

The counting number of the packet received.

Tx Collision:

Number of collisions transmitting frames experienced.

Rx Error Packet:

Number of bad packets received.

3-2-4. Detail Counter

The function of Detail Counter collects any information and provides the counting about the traffic of the port, no matter the packet is good or bad.

In the Fig. 3-14, the window can show only one port counter information at the same time. To see another port's counter, you have to pull down the list of Select, then you will see the figures displayed about the port you had chosen.

Each data field has 20-digit long. If the counting is overflow, the counter will be reset and restart counting. The data is updated every time interval defined by the user. The valid range is 3 to 10 seconds. The Refresh Interval is used to set the update frequency. Default update time is 3 seconds.

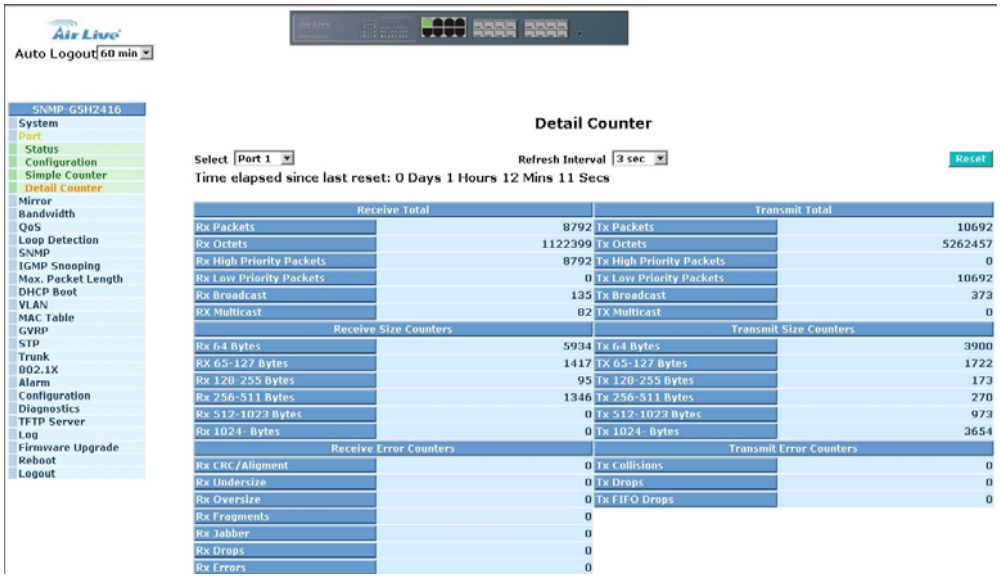


Fig. 3-14

Function name:

Detail Counter

Function description:

Display the detailed counting number of each port's traffic. In the Fig. 3-14, the window can show all counter information of each port at one time.

Parameter description:

Rx Packets:

The counting number of the packet received.

RX Octets:

Total received bytes.

Rx High Priority Packets:

Number of Rx packets classified as high priority.

Rx Low Priority Packets:

Number of Rx packets classified as low priority.

Rx Broadcast:

Show the counting number of the received broadcast packet.

Rx Multicast:

Show the counting number of the received multicast packet.

Tx Packets:

The counting number of the packet transmitted.

TX Octets:

Total transmitted bytes.

Tx High Priority Packets:

Number of Tx packets classified as high priority.

Tx Low Priority Packets:

Number of Tx packets classified as low priority.

Tx Broadcast:

Show the counting number of the transmitted broadcast packet.

Tx Multicast:

Show the counting number of the transmitted multicast packet.

Rx 64 Bytes:

Number of 64-byte frames in good and bad packets received.

Rx 65-127 Bytes:

Number of 65 ~ 126-byte frames in good and bad packets received.

Rx 128-255 Bytes:

Number of 127 ~ 255-byte frames in good and bad packets received.

Rx 256-511 Bytes:

Number of 256 ~ 511-byte frames in good and bad packets received.

Rx 512-1023 Bytes:

Number of 512 ~ 1023-byte frames in good and bad packets received.

Rx 1024-Bytes:

Number of 1024-max_length-byte frames in good and bad packets received.

Tx 64 Bytes:

Number of 64-byte frames in good and bad packets transmitted.

Tx 65-127 Bytes:

Number of 65 ~ 126-byte frames in good and bad packets transmitted.

Tx 128-255 Bytes:

Number of 127 ~ 255-byte frames in good and bad packets transmitted.

Tx 256-511 Bytes:

Number of 256 ~ 511-byte frames in good and bad packets transmitted.

Tx 512-1023 Bytes:

Number of 512 ~ 1023-byte frames in good and bad packets transmitted.

Tx 1024-Bytes:

Number of 1024-max_length-byte frames in good and bad packets transmitted.

Rx CRC/Alignment:

Number of Alignment errors and CRC error packets received.

Rx Undersize:

Number of short frames (<64 Bytes) with valid CRC.

Rx Oversize:

Number of long frames(according to max_length register) with valid CRC.

Rx Fragments:

Number of short frames (< 64 bytes) with invalid CRC.

Rx Jabber:

Number of long frames(according tomax_length register) with invalid CRC.

Rx Drops:

Frames dropped due to the lack of receiving buffer.

Rx Errors:

Number of the error packet received.

Tx Collisions:

Number of collisions transmitting frames experienced.

Tx Drops:

Number of frames dropped due to excessive collision, late collision, or frame aging.

Tx FIFO Drops:

Number of frames dropped due to the lack of transmitting buffer.

3-3. Mirror

Function name:

Mirror Configuration

Function description:

Mirror Configuration is to monitor the traffic of the network. For example, we assume that Port A and Port B are Monitoring Port and Monitored Port respectively, thus, the traffic received by Port B will be copied to Port A for monitoring.

Note:

When configuring the mirror function, you should avoid setting a port to be a sniffer port and aggregated port at the same time. It will cause something wrong.

Parameter description:

Mode:

Used for the activation or de-activation of Port Mirror function. Default is disable.

Monitoring Port:

Set up the port for monitoring. Valid port is Port 1~24 and default is Port 1.

Monitored Port:

Set up the port for being monitored. Just tick the check box (☑) beside the port x and valid port is Port 1~24.

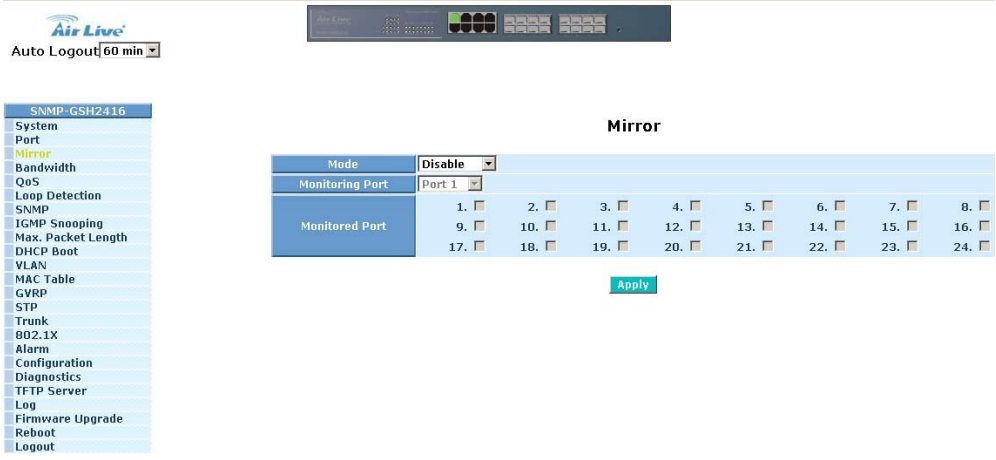


Fig. 3-15

3-4. Bandwidth Management

Function name:

Bandwidth Management

Function description:

Bandwidth Management function is used to set up the limit of Ingress and Egress bandwidth for each port.

Note:

Each port of the switch owns 16KB packet buffer. The packet buffer size will be reduced when the bandwidth rate limitation is enabled, which may cause that jumbo frame cannot be forwarded.

Please avoid enabling jumbo frame and bandwidth rating functions at the same time.

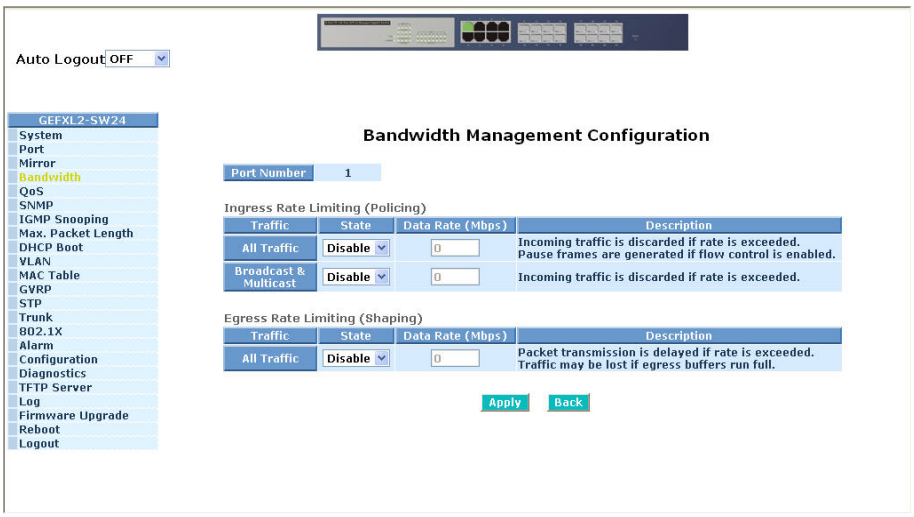


Fig. 3-16

Parameter description:

Port Number:

Choose the port that you would like this function to work on it. Valid range of the port is 1~24.

All Traffic for Ingress Rate Limiting(Policing):

Set up the limit of Ingress bandwidth for the port you choose. Incoming traffic will be discarded if the rate exceeds the value you set up in Data Rate field. Pause frames are also generated if flow control is enabled. The format of the packet limits to unicast, broadcast and multicast. Valid range is 0~1000.

Broadcast & Multicasat for Ingress Rate Limiting (Policing):

Set up the limit of Ingress bandwidth for the port you choose. Incoming traffic will be discarded if the rate exceeds the value you set up in Data Rate field. The format of the packet limits to broadcast and multicast. Valid range is 0~1000.

All Traffic for Egress Rate Limiting(Shaping):

Set up the limit of Egress bandwidth for the port you choose. Packet transmission will be delayed if the rate exceeds the value you set up in Data Rate field. Traffic may be lost if egress buffers run full. The format of the packet limits to unicast, broadcast and multicast. Valid range is 0~1000.

3-5. QoS(Quality of Service) Configuration

The switch offers powerful 5 kinds of QoS functions. There are Per Port Priority that you can assign each port to different precedence, VLAN Tag priority that can make precedence of 8 priorities, IP TOS Classification, IP TCP/UDP Port Classification and IP DiffServe Classification.

In Quality of Service (QoS) Configuration, there is one option named" Default Class". As you had selected one of the five QoS functions, then some packets that did not belong to this QoS setting would be viewed as Default Class. For instance, if you set QoS function as VLAN Tag Priority mode, and then choose Default Class as High, finally, the priority of the packets with no tag will be considered as High priority precedence. The initial value of the Default Class is High.

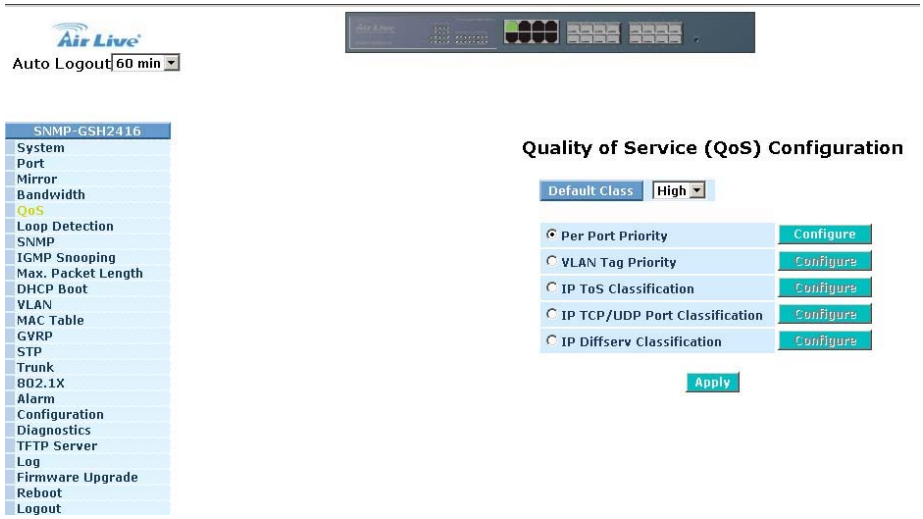


Fig. 3-17

Function name:

Per Port Priority

Function description:

We can assign QoS Priority, including High and Low for each port. For example, if we transmit IP packets from Port 2 and Port 3 at the speed of 1Gbps to Port 1, and set the Class of Port 2 as High and Port 3 as Low, then the packets of Port 3 will be dropped when the congestion happens because Port 2 owns higher precedence of transmitting packets.

Parameter description:

Port No:

User can choose the port (1~24) respectively with Priority Class on Per Port Priority function.

Class:

User can set up High Priority or Low Priority for each port respectively.

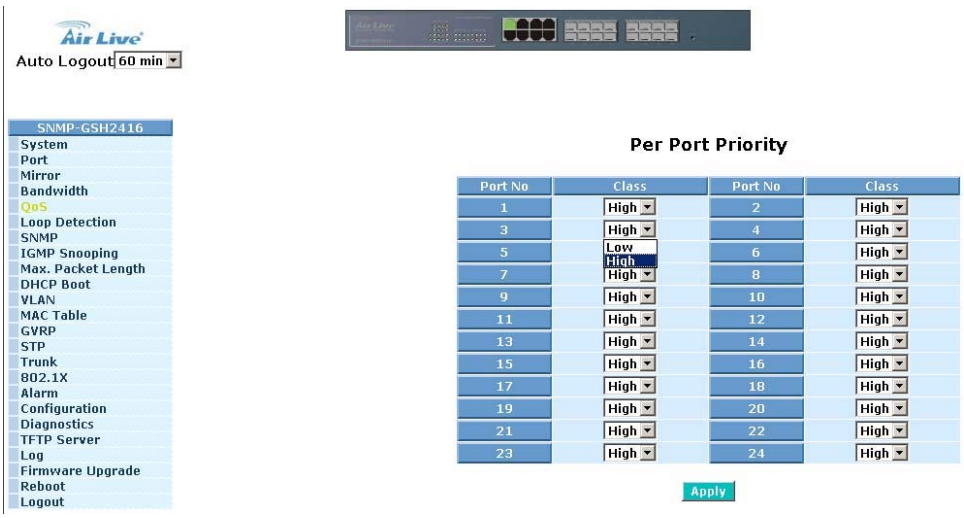


Fig. 3-18

Function name:

VLAN Tag Priority

Function description:

In vlan tag, there are 3 bits belonging to priority. According to these 3 bits, we could arrange 8 traffics –0 0 0, 0 0 1, 0 1 0, 0 1 1, 1 0 0, 1 0 1, 1 1 0, 1 1 1. We can set High priority or Low priority for each traffic class. For instance, if we let VLAN-tagged priority 0 0 0 be high priority and VLAN-tagged priority 0 0 1 be Low Priority, and then make port 1, 2, 3 be in the vlan 2. We sent the packets that have the value 0 0 0 in vlan-tagged field and VID equals 2 from the port 2 and the packets that have the value 0 0 1 in vlan-tagged field and VID equals 2 from the port 3 into the switch. We let the two kinds of packets be transmitted for port 1 until the port results in congestion. The result is that the packets will be dropped partially from the port 3 because the packets that belong to Low Priority. For the use of VLAN Tag Priority function, please press **<Configure>** button at the right section for setting in advance.

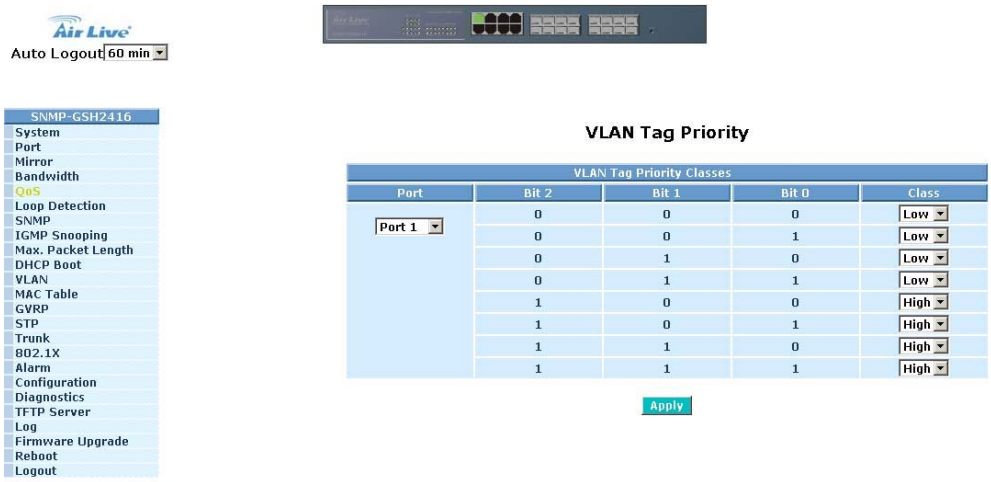


Fig. 3-19

Parameter description:

Quality of Service (QoS) Vlan Tag Configuration:

Used for setting up the QoS belongs to Vlan operation.

Port:

User can set up the port (1~24) respectively to let Vlan Tag QoS function work on them. If you would like to set up all ports at a time, user is also allowed to choose “All” in the selection list to simplify the procedure of configuration.

Bit 0, Bit 1, Bit 2:

According to the arrangement of VLAN-tagged priority, it can form 8 kinds of traffics, including 0 0 0, 0 0 1, 0 1 0, 0 1 1, 1 0 0, 1 0 1, 1 1 0 and 1 1 1.

Class:

8 kinds of traffic as mentioned above, user can set up High Priority or Low Priority for each port respectively.

Function name:

IP ToS Classification

Function description:

Another QoS function is the application of Layer 3 on network framework. We focus on TOS field of IP header. There are three bits in TOS field. We means bit 5~7 of TOS field that we will use. According to these 3 bits, we could arrange 8 traffics –0 0 0, 0 0 1, 0 1 0, 0 1 1, 1 0 0, 1 0 1, 1 1 0, 1 1 1. As long as we change bit 5~7 of TOS field of IP header, we will create the 8 traffic packets we meant before. Moreover, we can set High priority or Low priority for each traffic class. For instance, if we let TOS 0 0 0 be high priority and TOS 0 0 1 be Low Priority, we sent in the packets that have bit 5~7 of TOS Field appears 0 0 0 from the port 2 and the packets that have bit 5~7 of TOS Field appears 0 0 1 from the port 3. We let the two kinds of packets be transmitted for port 1 until the port results in congestion. The result is that the packets will be dropped partially from the port 3 because the packets that belong to Low Priority.

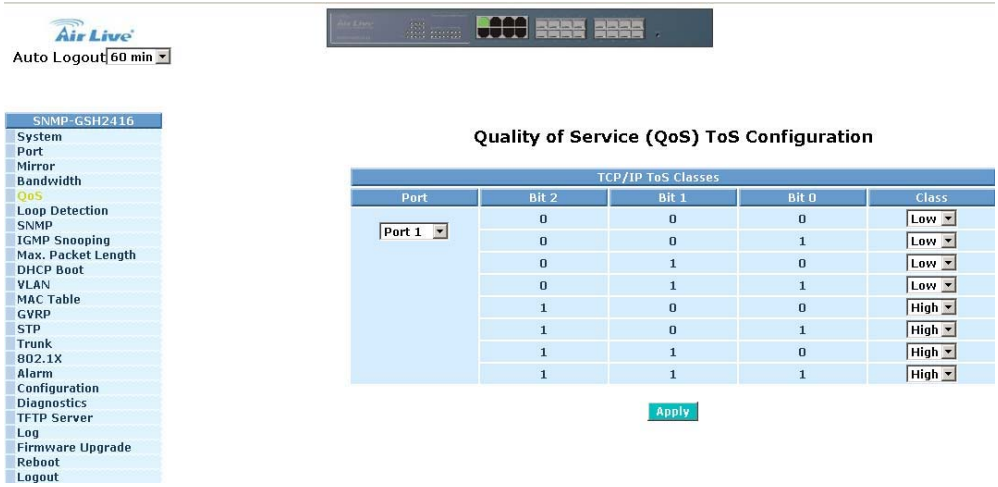


Fig. 3-20

Parameter description:

Quality of Service (QoS) ToS Configuration:

Used for setting up the QoS in Layer 3.

Port:

User can set up the port (1~24) respectively to let TOS QoS function work on them. If you would like to set up all ports at a time, user is also allowed to choose “All” in the selection list to simplify the procedure of configuration.

Bit 0, Bit 1, Bit 2:

According to the arrangement of Bit 5 ~ Bit 7 in TOS Field of IP Header, it can form 8 kinds of traffics, including 0 0 0, 0 0 1, 0 1 0, 0 1 1, 1 0 0, 1 0 1, 1 1 0 and 1 1 1.

Class:

8 kinds of traffic as mentioned above, user can set up High Priority or Low Priority for each port respectively.

Function name:

IP TCP/UDP Port Classification

Function description:

In L4 QoS Configuration, you can enter one of these special network transmission events, for example we use" Down prioritize web browsing, e-mail, FTP and news "L4 QoS Configuration and click **<Apply>** button, and then click **<Advance** >>**>** button. We can find Special TCP/UDP port 80, 280, 443, 25, 110, 20, 21, 69, 119, 2009 have already existed and defined for your using but it is fine that you modify this pre-defined TCP/UDP port with other port number you prefer. In " Down prioritize web browsing, e-mail, FTP and news " L4 QoS Configuration with default setting, special defined TCP/UDP port possesses lower QoS traffic than Default class (all other TCP/UDP ports such as port 81,82,83,84,85, etc.). Giving an example, when we transmit TCP packets with port number 80 at each of port 2 and port number 81 at port 3 to port 1 until the congestion happens. The packets from port 3 will be dropped by port 1 because the TCP packets have port number 80 is high priority and will have higher precedence to be sent out from port 1.

Parameter description:

Disable IP TCP/UDP Port Classification:

Belong to the QoS in L4. Just tick the option button and press **<Apply>** button to have this function taken affect. Then, click **<Advance** >>**>** button to set up Special TCP/UDP port for QoS.

Down prioritize web browsing, e-mail, FTP and news:

Belong to the QoS in L4. Just tick the option button and press **<Apply>** button to have this function taken affect. Then, click **<Advance** >>**>** button to set up Special TCP/UDP port for QoS.

Prioritize IP Telephony (VoIP):

Belong to the QoS in L4. Just tick the option button and press **<Apply>** button to have this function taken affect. Then, click **<Advance** >>**>** button set up Special TCP/UDP port for QoS.

Prioritize iSCSI:

Belong to the QoS in L4. Just tick the option button and press **<Apply>** button to have this function taken affect. Then, click **<Advance** >>**>** button to set up Special TCP/UDP port for QoS.

Prioritize web browsing, e-mail, FTP transfers and news:

Belong to the QoS in L4. Just tick the option button and press **<Apply>** button to have this function taken affect. Then, click **<Advance** >>**>** button to set up Special TCP/UDP port for QoS.

Prioritize Streaming Audio/Video:

Belong to the QoS in L4. Just tick the option button and press **<Apply>** button to have this function taken affect. Then, click **<Advance >>>** button set up Special TCP/UDP port for QoS.

Prioritize Databases (Oracle, IBM DB2, SQL, Microsoft):

Belong to the QoS in L4. Just tick the option button and press **<Apply>** button to have this function taken affect. Then, click **<Advance >>>** button to set up Special TCP/UDP port for QoS.

Advanced Mode:

Display the TCP/UDP port number in L4 QoS. In “Disable IP TCP/UDP Port Classification” mode, user can randomly choose TCP/UDP port number that L4 QoS will affect. As to other special L4 QoS events, Special TCP/UDP port number will be took action. Of course, user could be allowed to add or modify the port number at random. For instance, if we choose “Down prioritize web browsing, e-mail, FTP and news” as the QoS of L4 and enter the “Advanced Mode”, then we can see that some special port number 80, 280, 443, 25, 110, 20, 21, 69, 119, 2009 have been configured already. User also has the right to modify these port numbers. The display is shown as Fig. 3-21.

Special TCP/UDP class:

There are two modes for selection, including Low and High.

Default class (all other TCP/UDP ports):

There are two modes for selection, including Low and High.

Port:

User can set up the port (1~24) respectively to let Special TDP/UDP class function work on them. If you would like to set up all ports at a time, user is allowed to choose “All” selection to simplify the procedure of configuration.

Special UDP/TCP Port Selection:

The following are port numbers defined by six specific networks in L4:

- Down prioritize web browsing, e-mail, FTP and news: port number 80,280,443,25,110,20,21,69,119,2009
- Prioritize IP Telephony (VoIP):1718,1719,1720
- Prioritize iSCSI:3225,3260,3420
- Prioritize web browsing, e-mail, FTP transfers and news: 80,280,443,25,110,20,21,69,119,2009
- Prioritize Streaming Audio/Video: 2979,1755,7070,7071,554,8000
- Prioritize Databases (Oracle, IBM DB2, SQL, Microsoft): 66,1571,1575,523,118,156,3306,1232,1433,1434

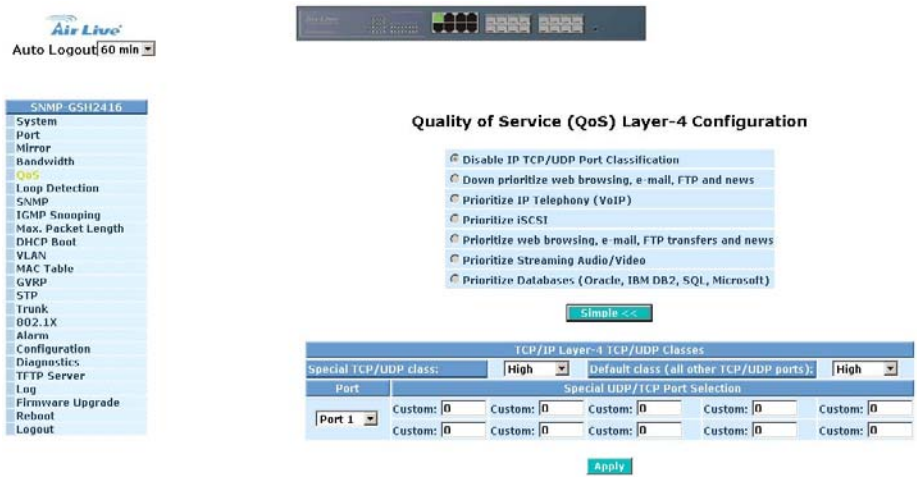


Fig. 3-21 Advanced Mode

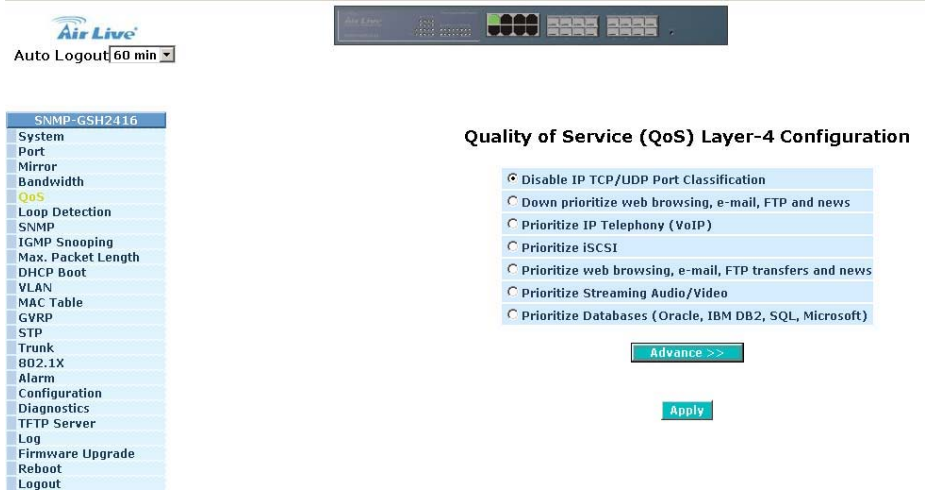


Fig. 3-22 Simple Mode

Simple Mode:

Press **<Simple<<>** button is to return to the screen that all L4 port number will disappear (See Fig. 3-22).

Function name:

IP Diffserv Classification

Function description:

In the late 1990s, the IETF redefined the meaning of the 8-bit SERVICE TYPE field to accommodate a set of differentiated services (DS). Under the differentiated services interpretation, the first six bits comprise a codepoint, which is sometimes abbreviated DSCP, and the last two bits are left unused.

IP Diffserve Classification function, it can form total 64 (0~63) kinds of Traffic Class based on the arrangement of 6-bit field in DSCP of the IP packet. In the switch, user is allowed to set up these 64 kinds of Class that belong to High or Low Priority.

Parameter description:

IP Differentiated Services (DiffServ) Configuration:

Used for setting up the IP Differentiated Services Configuration QoS.

Diffserv:

Display 64 (0~63) DiffServ Priority items.

Class:

64 kinds of traffic as we mentioned above, user can set up High Priority or Low Priority for each port respectively.

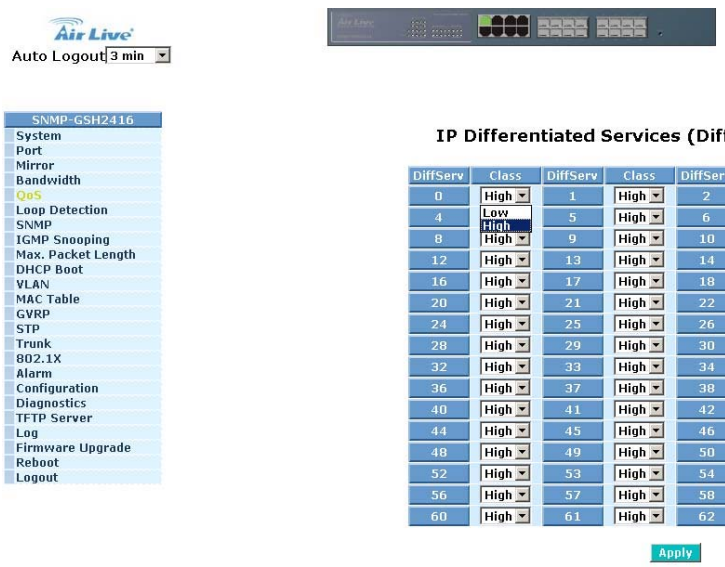


Fig. 3-23

3-6. SNMP Configuration

Any Network Management System (NMS) running the Simple Network Management Protocol (SNMP) can manage the Managed devices equipped with SNMP agent, provided that the Management Information Base (MIB) is installed correctly on the managed devices. The SNMP is a protocol that is used to govern the transfer of information between SNMP manager and agent and traverses the Object Identity (OID) of the management Information Base (MIB), described in the form of SMI syntax. SNMP agent is running on the switch to response the request issued by SNMP manager.

Basically, it is passive except issuing the trap information. The switch supports a switch to turn on or off the SNMP agent. If you set the field SNMP "Enable", SNMP agent will be started up. All supported MIB OIDs, including RMON MIB, can be accessed via SNMP manager. If the field SNMP is set "Disable", SNMP agent will be de-activated, the related Community Name, Trap Host IP Address, Trap and all MIB counters will be ignored.

Function name:

SNMP Configuration

Function description:

This function is used to configure SNMP settings, community name, trap host and public traps as well as the throttle of SNMP. A SNMP manager must pass the authentication by identifying both community names, then it can access the MIB information of the target device. So, both parties must have the same community name. Once completing the setting, click **<Apply>** button, the setting takes effect.

Parameters description:

SNMP:

The term SNMP here is used for the activation or de-activation of SNMP. Default is Enable.

Get/Set/Trap Community:

Community name is used as password for authenticating if the requesting network management unit belongs to the same community group. If they both don't have the same community name, they don't belong to the same group. Hence, the requesting network management unit can not access the device with different community name via SNMP protocol; If they both have the same community name, they can talk each other.

Community name is user-definable with a maximum length of 15 characters and is case sensitive. There is not allowed to put any blank in the community name string. Any printable character is allowable.

The community name for each function works independently. Each function has its own community name. Say, the community name for GET only works for GET function and can't be applied to other function such as SET and Trap.

Default SNMP function : Enable

Default community name for GET: public

Default community name for SET: private

Default community name for Trap: public

Default Set function : Enable

Default trap host IP address: 0.0.0.0

Default port number :162

Trap:

In the switch, there are 6 trap hosts supported. Each of them has its own community name and IP address; is user-definable. To set up a trap host means to create a trap manager by assigning an IP address to host the trap message. In other words, the trap host is a network management unit with SNMP manager receiving the trap message from the managed switch with SNMP agent issuing the trap message. 6 trap hosts can prevent the important trap message from losing.

For each public trap, the switch supports the trap event Cold Start, Warm Start, Link Down, Link Up and Authentication Failure Trap. They can be enabled or disabled individually. When enabled, the corresponded trap will actively send a trap message to the trap host when a trap happens. If all public traps are disabled, no public trap message will be sent. As to the Enterprise (no. 6) trap is classified as private trap, which are listed in the Trap Alarm Configuration function folder.

Default for all public traps: Enable.

Fig. 3-24 Community and trap host setting

3-7. IGMP Snooping

The function, IGMP Snooping, is used to establish the multicast groups to forward the multicast packet to the member ports, and, in nature, avoids wasting the bandwidth while IP multicast packets are running over the network. This is because a switch that does not support IGMP or IGMP Snooping can not tell the multicast packet from the broadcast packet, so it can only treat them all as the broadcast packet. Without IGMP Snooping, the multicast packet forwarding function is plain and nothing is different from broadcast packet.

A switch supported IGMP Snooping with the functions of query, report and leave, a type of packet exchanged between IP Multicast Router/Switch and IP Multicast Host, can update the information of the Multicast table when a member (port) joins or leaves an IP Multicast Destination Address. With this function, once a switch receives an IP multicast packet, it will forward the packet to the members who joined in a specified IP multicast group before.

The packets will be discarded by the IGMP Snooping if the user transmits multicast packets to the multicast group that had not been built up in advance.

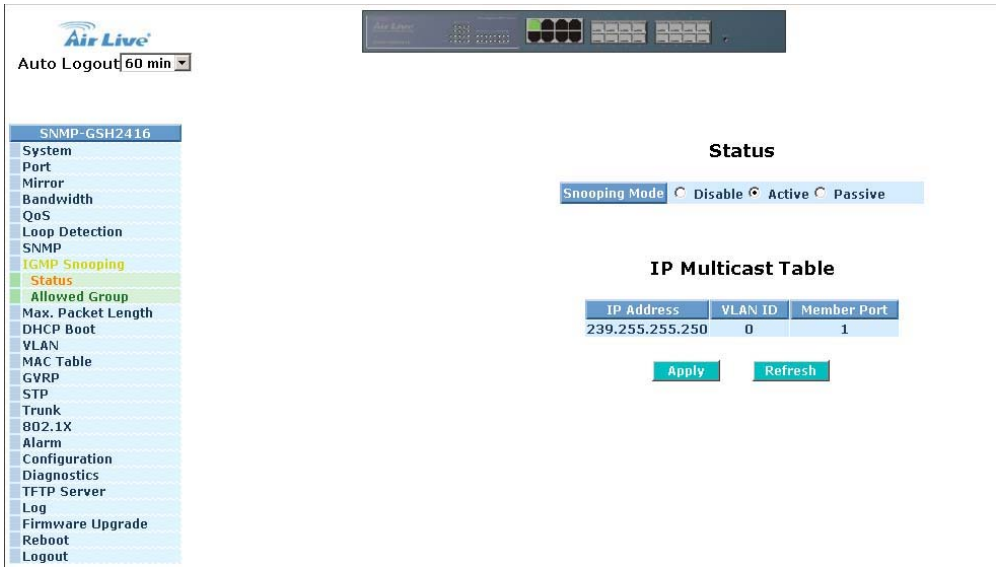


Fig. 3-25

Function name:

IGMP Snooping Status

Function description:

IGMP is used to snoop the status of IP multicast groups and display its associated information in both tagged VLAN and non-tagged VLAN networks. Enabling IGMP with either passive or active mode, you can monitor the IGMP snooping information, which contains the multicast member list with the multicast groups, VID and member port.

Parameter description:

IGMP snooping mode selection:

The switch supports three kinds of IGMP Snooping status, including “Passive”, “Active” and “Disable”.

Disable:

Set “Disable” mode to disable IGMP Snooping function.

Default: Disable

Active:

In Active mode, IGMP snooping switch will periodically issue the Membership Query message to all hosts attached to it and gather the Membership report message to update the database of the Multicast table. By the way, this also reduces the unnecessary multicast traffic.

Passive:

In Passive Snooping mode, the IGMP snooping will not periodically poll the hosts in the groups. The switch will send a Membership Query message to all hosts only when it has received a Membership Query message from a router.

IP Address:

Show all multicast groups IP addresses that are registered on this device.

VLAN ID:

Show VLAN ID for each multicast group.

Member Port:

Show member ports that join each multicast group. Member port may be only or more than one.

Function name:

Allowed Group

Function description:

The Allowed Group function allows the IGMP Snooping to set up the IP multicast table based on user's specific conditions. IGMP report packets that meet the items you set up will be joined or formed the multicast group.

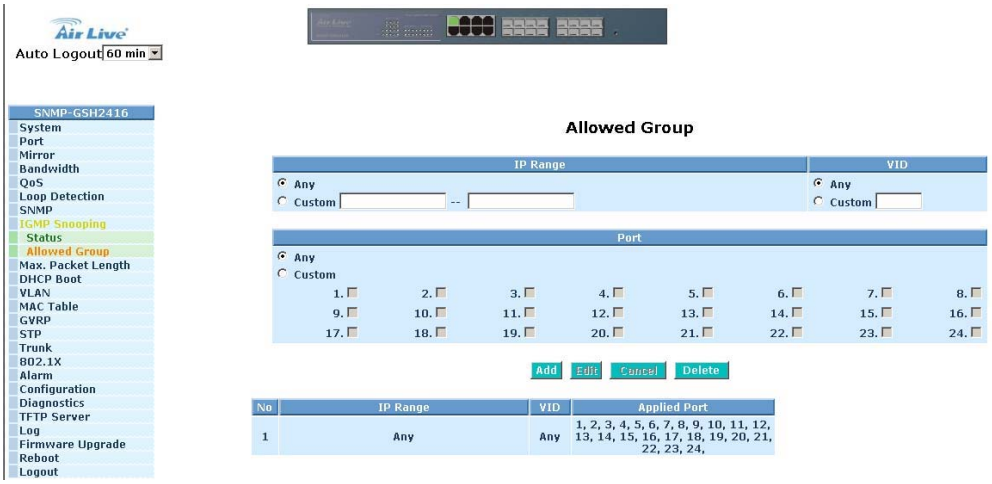


Fig. 3-26

Parameter description:

IP Range:

The switch supports two kinds of options for managed valid IP range, including "Any" and "Custom". Default is "Any". In case that" Custom" had been chosen, you can assigned effective IP range. The valid range is 224.0.0.0~239.255.255.255.

VID:

The switch supports two kinds of options for managed valid VLAN VID, including "Any" and "Custom". Default is "Any". When you choose "Custom", you can fill in VID number. The valid VID range is 1~4094.

Port:

The switch supports two kinds of options for managed valid port range, including "Any" and "Custom". Default is "Any". You can select the ports that you would like them to be worked and restricted in the allowed group configuration if "Custom" had been chosen.

Add:

A new entry of allowed group configuration can be created after the parameters as mentioned above had been setup and then press **<Add>** button.

Edit:

The existed entry also can be modified after pressing **<Edit>** button.

Delete:

Remove the existed entry of allowed group configuration from the allowed group.

3-8. Max. Packet Length

Function name:

Max. Packet Length

Function description:

The switch is capable of dealing with 9k Jumbo Frames, which suits the transmission for a large amount of data in the network environment.

Parameter description:

Jumbo Frame(bytes):

Set up the maximum length of the packet that each port of the switch can accept. Maximum length can be up to 1532 bytes or 9216 bytes. The default is 1532 bytes.

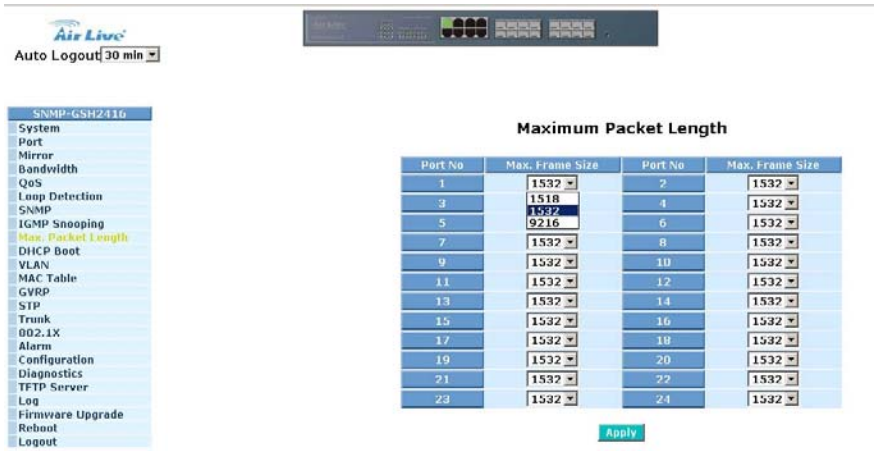


Fig. 3-27

3-9. DHCP Boot

The DHCP Boot function is used to spread the request broadcast packet into a bigger time frame to prevent the traffic congestion due to broadcast packets from many network devices which may seek its NMS, boot server, DHCP server and many connections predefined when the whole building or block lose the power and then reboot and recover. At this moment, a bunch of switch or other network device on the LAN will try its best to find the server to get the services or try to set up the predefined links, they will issue many broadcast packets in the network.

The switch supports a random delay time for DHCP and boot delay for each device. This suppresses the broadcast storm while all devices are at booting stage in the same time. The maximum user-defined delay time is 30 sec. If DHCP Broadcasting Suppression function is enabled, the delay time is set randomly, ranging from 0 to 30 seconds, because the exactly delay time is computed by the switch itself. The default is “Disable”.

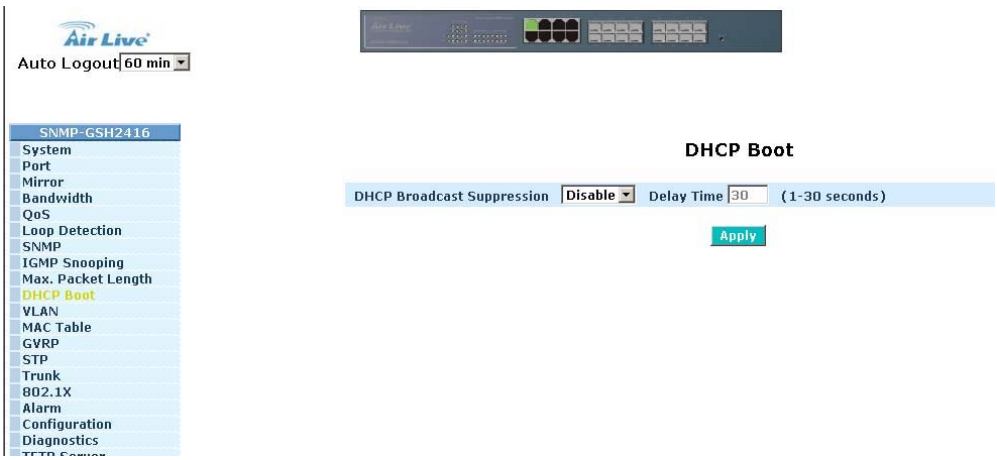


Fig. 3-28

3-10. VLAN

The switch supports Tag-based VLAN (802.1q) and Port-based VLAN. Support 256 active VLANs and VLAN ID 1~4094. VLAN configuration is used to partition your LAN into small ones as your demand. Properly configuring it, you can gain not only improving security and increasing performance but greatly reducing VLAN management.

3-10-1. VLAN Mode

Function name:

VLAN Mode Setting

Function description:

The VLAN Mode Selection function includes five modes: Port-based, Tag-based, Metro Mode, Double-tag and Disable, you can choose one of them by pulling down list and selecting an item. Then, click **<Apply>** button, the settings will take effect immediately.

Parameter description:

VLAN Mode:

Disable:

Stop VLAN function on the switch. In this mode, no VLAN is applied to the switch. This is the default setting.

Port-based:

Port-based VLAN is defined by port. Any packet coming in or outgoing from any one port of a port-based VLAN will be accepted. No filtering criterion applies in port-based VLAN. The only criterion is the physical port you connect to. For example, for a port-based VLAN named PVLAN-1 contains port members Port 1&2&3&4. If you are on the port 1, you can communicate with port 2&3&4. If you are on the port 5, then you cannot talk to them. Each port-based VLAN you built up must be assigned a group name. This switch can support up to maximal 24 port-based VLAN groups.

Tag-based:

Tag-based VLAN identifies its member by VID. This is quite different from port-based VLAN. If there are any more rules in ingress filtering list or egress filtering list, the packet will be screened with more filtering criteria to determine if it can be forwarded. The switch supports supplement of 802.1q. For more details, please see the section VLAN in Chapter 3.

Each tag-based VLAN you built up must be assigned VLAN name and VLAN ID. Valid VLAN ID is 1-4094. User can create total up to 64 Tag VLAN groups.

Metro Mode:

The Metro Mode is a quick configuration VLAN environment method on Port-based VLAN. It will create 22 or 23 Port-based VLAN groups.

Double-tag:

Double-tag mode belongs to the tag-based mode, however, it would treat all frames as the untagged ones, which means that tag with PVID will be added into all packets. Then, these packets will be forwarded as Tag-based VLAN. So, the incoming packets with tag will become the double-tag ones.

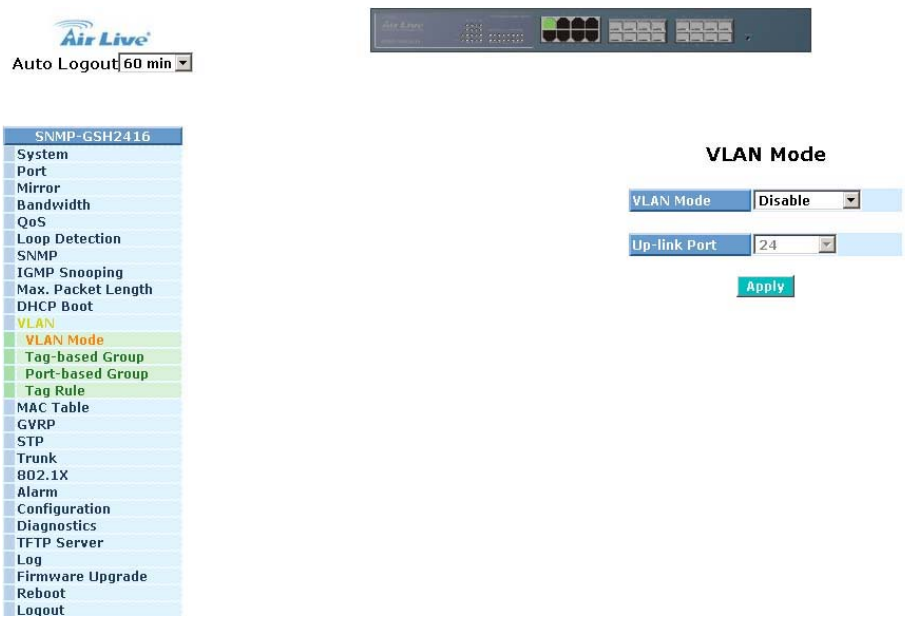


Fig. 3-29

Up-link Port:

This function is enabled only when metro mode is chosen in VLAN mode.

23:

Except Port 23, each port of the switch cannot transmit packets with each other. Each port groups a VLAN with Port 23, thus, total 23 groups consisting of 2 members are formed.

24:

Except Port 24, each port of the switch cannot transmit packets with each other. Each port groups a VLAN with Port 24, thus, total 23 groups consisting of 2 members are formed.

23&24:

Except Port 23 and Port 24, each port of the switch cannot transmit packets with each other. Each port groups a VLAN with Port 23 and Port 24, thus, total 22 groups consisting of 3 members are formed.

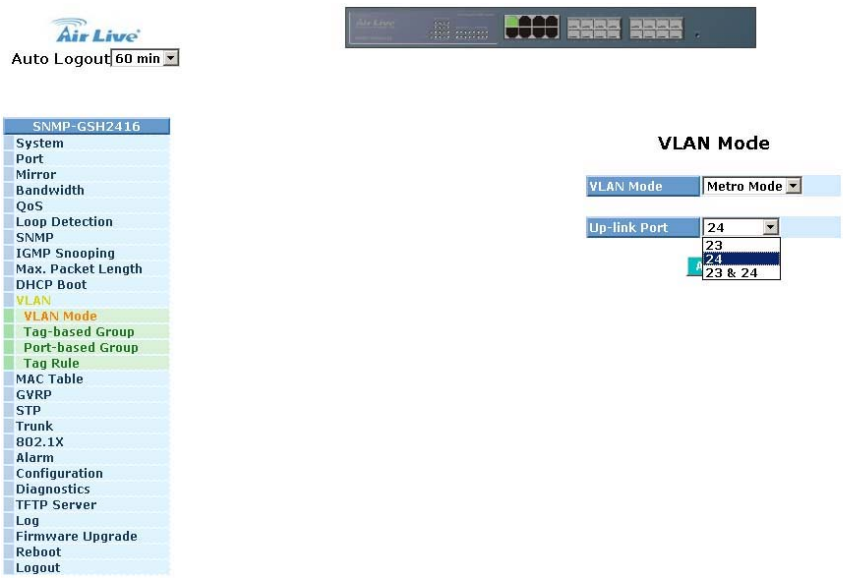


Fig. 3-30

3-10-2. Tag-based Group

Function name:

Tag-based Group Configuration

Function description:

It shows the information of existed Tag-based VLAN Groups, You can also easily create, edit and delete a Tag-based VLAN group by pressing **<Add>**, **<Edit>** and **<Delete>** function buttons. User can add a new VLAN group by inputting a new VLAN name and VLAN ID.

Parameter description:

VLAN Name:

The name defined by administrator is associated with a VLAN group. Valid letters are A-Z, a-z, 0-9, " - " and "_" characters. The maximal length is 15 characters.

VID:

VLAN identifier. Each tag-based VLAN group has a unique VID. It appears only in tag-based and Double-tag mode.

SYM-VLAN:

While the SYM-VLAN function of the group is enabled, all packets with this group VID will be dropped in case they are transmitted from the ports that do not belong to this group.

Member:

This is used to enable or disable if a port is a member of the new added VLAN, "Enable" means it is a member of the VLAN. Just tick the check box (☑) beside the port x to enable it.

Fig. 3-31

Add Group:

Create a new Tag-based VLAN. Input the VLAN name as well as VID, configure the SYM-VLAN function and choose the member by ticking the check box beside the port No., then, press the **<Apply>** button to have the setting taken effect.

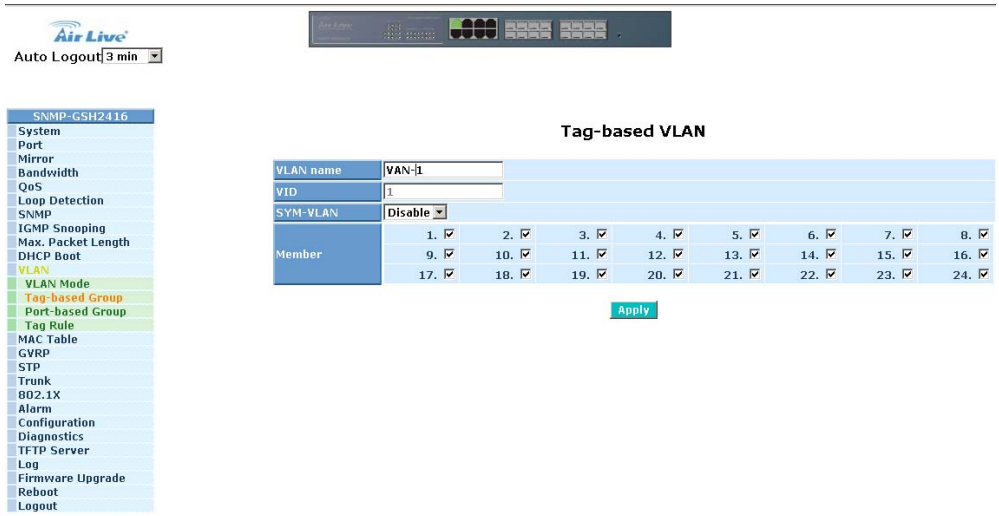


Fig. 3-32

Delete Group:

Just press the **<Delete>** button to remove the selected group entry from the Tag-based group table.

Fig. 3-33

Edit a group:

Just select a group entry and press the **<Edit>** button, then you can modify a group's description, SYM-VLAN and member set.

3-10-3. Port-based Group

Function name:

Port-based Group Configuration

Function description:

It shows the information of the existed Port-based VLAN Groups. You can easily create, edit and delete a Port-based VLAN group by pressing **<Add>**, **<Edit>** and **<Delete>** function buttons. User can add a new VLAN group by inputting a new VLAN name.

Parameter description:

VLAN Name:

The name defined by administrator is associated with a VLAN group. Valid letters are A-Z, a-z, 0-9, " - " and "_" characters. The maximal length is 15 characters.

Member:

This is used to enable or disable if a port is a member of the new added VLAN, "Enable" means it is a member of the VLAN. Just tick the check box (☑) beside the port x to enable it.

Fig. 3-34

Add Group:

Create a new Port-based VLAN. Input the VLAN name and choose the member by ticking the check box beside the port No., then, press the **<Apply>** button to have the setting taken effect.

Fig. 3-35

Delete Group:

Just press the **<Delete>** button to remove the selected group entry from the Port-based group table.

Fig. 3-36

Edit a group:

Just select a group entry and press the **<Edit>** button, then you can modify a group‘s description and member set.

3-10-4. Tag Rule

Function name:

Tag Rule

Function description:

In VLAN Tag Rule Setting, user can input VID number to each port. The range of VID number is from 1 to 4094. User also can choose ingress filtering rules to each port. There are two ingress filtering rules which can be applied to the switch. The Ingress Filtering Rule 1 is “forward only packets with VID matching this port’s configured VID”. The Ingress Filtering Rule 2 is “drop untagged frame”. You can also select the Role of each port as Access, Trunk, or Hybrid.

Parameter description:

Port 1-24:

Port number.

PVID:

This PVID range will be 1-4094. Before you set a number x as PVID, you have to create a Tag-based VLAN with VID x. For example, if port x receives an untagged packet, the switch will apply the PVID (assume as VID y) of port x to tag this packet, the packet then will be forwarded as the tagged packet with VID y.

Rule 1:

Forward only packets with VID matching this port’s configured VID. You can apply Rule 1 as a way to a given port to filter unwanted traffic. In Rule 1, a given port checks if the given port is a member of the VLAN on which the received packet belongs to, to determine forward it or not. For example, if port 1 receives a tagged packet with VID=100 (VLAN name=VLAN100), and if Rule 1 is enabled, the switch will check if port 1 is a member of VLAN100. If yes, the received packet is forwarded; otherwise, the received packet is dropped.

Rule 2:

Drop untagged frame. You can configure a given port to accept all frames (Tagged and Untagged) or just receive tagged frame. If the former is the case, then the packets with tagged or untagged will be processed. If the later is the case, only the packets carrying VLAN tag will be processed, the rest packets will be discarded.

Note: If Rule 1 is enabled and port 1, for example, receives an untagged packet, the switch will apply the PVID of port 1 to tag this packet, the packet then will be forwarded. But if the PVID of port 1 is 100 and port 1 is not member of VLAN 100, the packet will be dropped.

Role:

This is an egress rule of the port. Here you can choose Access, Trunk or Hybrid. Trunk means the outgoing packets must carry VLAN tag header. Access means the outgoing packets carry no VLAN tag header. If packets have double VLAN tags, one will be dropped and the other will still be left. As to Hybrid, it is similar to Trunk, and both of them will tag-out. When the port is set to Hybrid, its packets will be untagged out if the VID of the outgoing packets with tag is the same as the one in the field of Untag VID of this port.

Untag VID:

Valid range is 1~4094. It works only when Role is set to Hybrid.

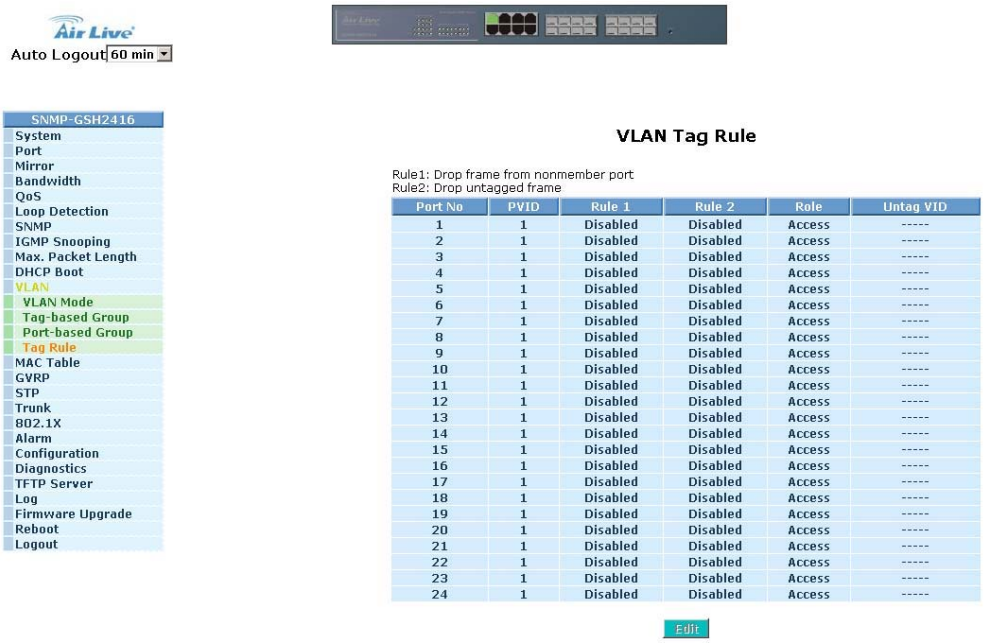

Air Live
Auto Logout 60 min
SNMP-GSH2416
System
Port
Mirror
Bandwidth
QoS
Loop Detection
SNMP
IGMP Snooping
Max. Packet Length
DHCP Boot
VLAN
VLAN Mode
Tag-based Group
Port-based Group
Tag Rule
MAC Table
GVRP
STP
Trunk
802.1X
Alarm
Configuration
Diagnostics
TFTP Server
Log
Firmware Upgrade
Reboot
Logout
VLAN Tag Rule
Rule1: Drop frame from nonmember port
Rule2: Drop untagged frame
Port No | PVID | Rule 1 | Rule 2 | Role | Untag VID
1 | 1 | Disabled | Disabled | Access | -----
2 | 1 | Disabled | Disabled | Access | -----
3 | 1 | Disabled | Disabled | Access | -----
4 | 1 | Disabled | Disabled | Access | -----
5 | 1 | Disabled | Disabled | Access | -----
6 | 1 | Disabled | Disabled | Access | -----
7 | 1 | Disabled | Disabled | Access | -----
8 | 1 | Disabled | Disabled | Access | -----
9 | 1 | Disabled | Disabled | Access | -----
10 | 1 | Disabled | Disabled | Access | -----
11 | 1 | Disabled | Disabled | Access | -----
12 | 1 | Disabled | Disabled | Access | -----
13 | 1 | Disabled | Disabled | Access | -----
14 | 1 | Disabled | Disabled | Access | -----
15 | 1 | Disabled | Disabled | Access | -----
16 | 1 | Disabled | Disabled | Access | -----
17 | 1 | Disabled | Disabled | Access | -----
18 | 1 | Disabled | Disabled | Access | -----
19 | 1 | Disabled | Disabled | Access | -----
20 | 1 | Disabled | Disabled | Access | -----
21 | 1 | Disabled | Disabled | Access | -----
22 | 1 | Disabled | Disabled | Access | -----
23 | 1 | Disabled | Disabled | Access | -----
24 | 1 | Disabled | Disabled | Access | -----
Edit

Fig. 3-37

3-11. MAC Table

MAC Table Configuration gathers many functions, including MAC Table Information, MAC Table Maintenance, Static Forward, Static Filter and MAC Alias, which cannot be categorized to some function type. They are described below.

Function name:

MAC Table Information

Function Description:

Display the static or dynamic learning MAC entry and the state for the selected port.

Parameter description:

Port:

Select the port you would like to inquire.

Search:

Set up the MAC entry you would like to inquire.

The default is ??-??-??-??-??-??

MAC:

Display the MAC address of one entry you selected from the searched MAC entries table.

Alias:

Set up the Alias for the selected MAC entry.

Set Alias:

Save the Alias of MAC entry you set up.

Search:

Find the entry that meets your setup.

Previous Page:

Move to the previous page.

Next Page:

Move to the next page.

Alias:

The Alias of the searched entry.

MAC Address:

The MAC address of the searched entry.

Port:

The port that exists in the searched MAC Entry.

VID:

VLAN Group that MAC Entry exists.

State:

Display the method that this MAC Entry is built. It may show “Dynamic MAC” or “Static MAC”.

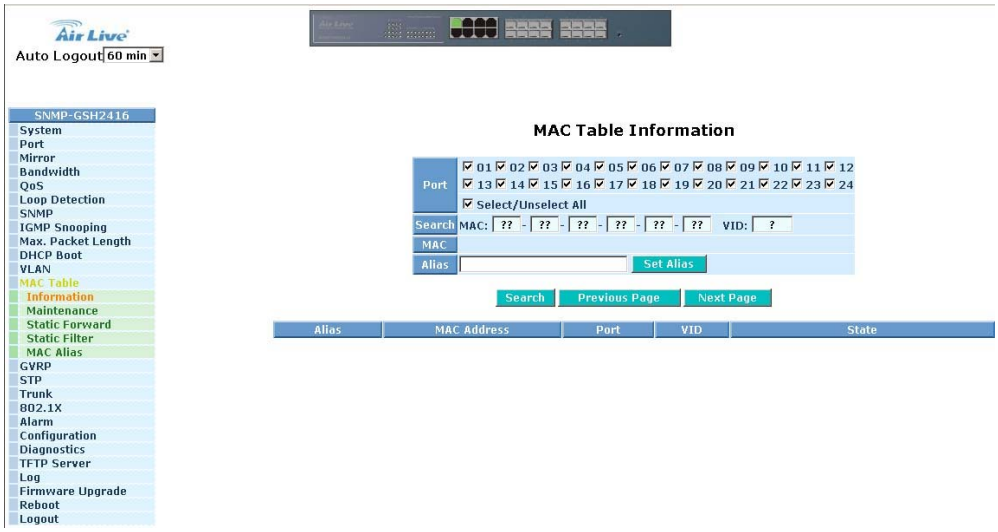


Fig. 3-38

Function Name:

MAC Table Maintenance

Function Description:

This function can allow the user to set up the processing mechanism of MAC Table. An idle MAC address exceeding MAC Address Age-out Time will be removed from the MAC Table. The range of Age-out Time is 10-65535 seconds, and the setup of this time will have no effect on static MAC addresses.

Parameter description:

Aging Time:

Delete a MAC address idling for a period of time from the MAC Table, which will not affect static MAC address. Range of MAC Address Aging Time is 10-65535 seconds. The default Aging Time is 300 seconds.

Flush:

Remove all entries that do not belong to the static Mac Entry from the MAC Table.

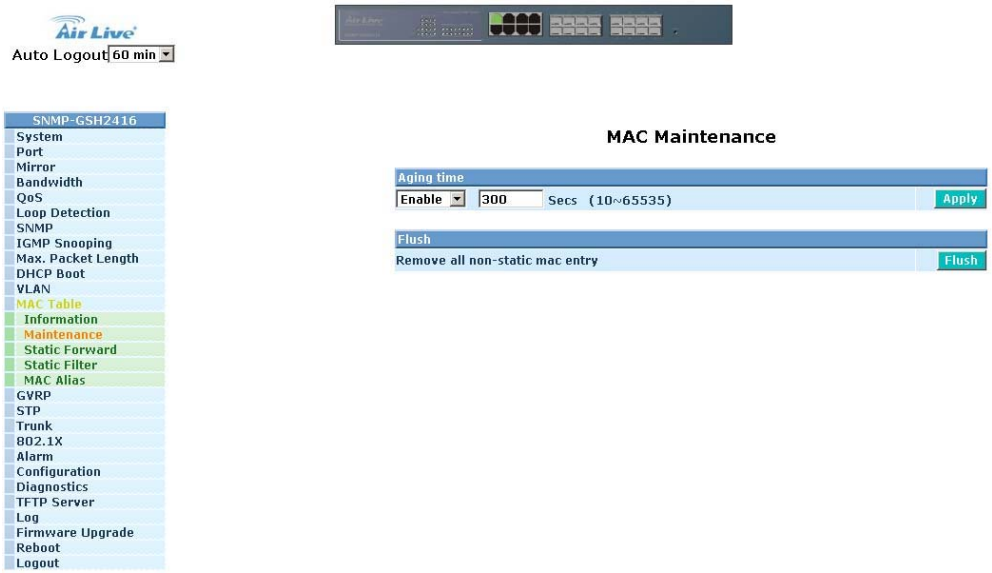


Fig. 3-39

Function Name:

Static Forward

Function Description:

Static Forward is a function that allows the user in the static forward table to access a specified port of the switch. Static Forward table associated with a specified port of a switch is set up by manually inputting MAC address and its alias name.

When a MAC address is assigned to a specific port, all of the switch's traffics sent to this MAC address will be forwarded to this port.

For adding a MAC address entry in the allowed table, you just need to fill in four parameters: MAC address, associated port, VID and Alias. Just select the existed MAC address entry you want and click **<Delete>** button, you also can remove it.

Parameter description:

MAC:

It is a six-byte long Ethernet hardware address and usually expressed by hex and separated by hyphens. For example,

00 – 40 - C7 - D6 – 00 - 01

Port No:

Port number of the switch. It is 1 ~24.

VID:

VLAN identifier. This will be filled only when tagged VLAN is applied. Valid range is 1 ~ 4094.

Alias:

MAC alias name you assign.

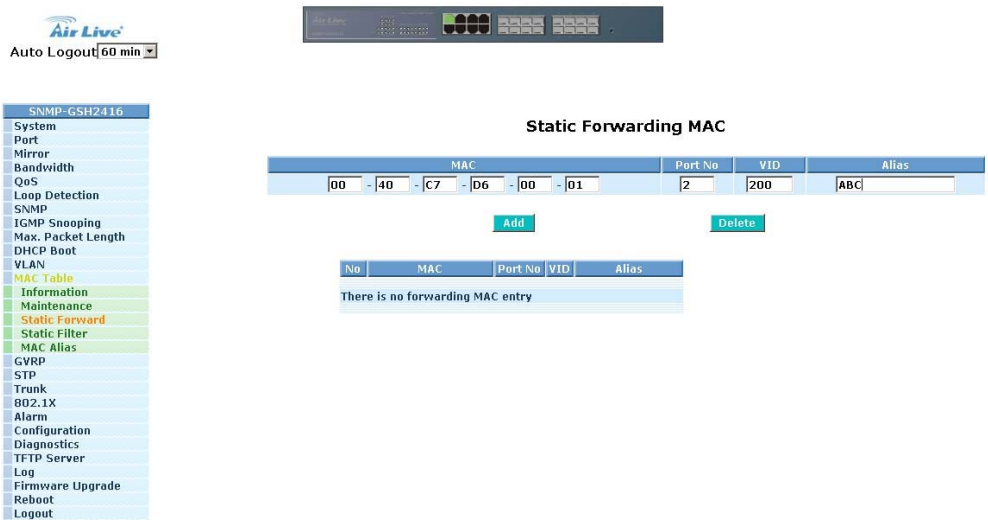


Fig. 3-40

Function name:

Static Filter

Function Description:

Static Filter is a function that denies the packet forwarding if the packet's MAC Address is listed in the filtering Static Filter table. User can very easily maintain the table by filling in MAC Address, VID (VLAN ID) and Alias fields individually. User also can delete the existed entry by clicking **<Delete>** button.

Parameter description:

MAC:

It is a six-byte long Ethernet hardware address and usually expressed by hex and separated by hyphens. For example,

00 – 40 - C7 - D6 – 00 - 02

VID:

VLAN identifier. This will be filled only when tagged VLAN is applied. Valid range is 1 ~ 4094.

Alias:

MAC alias name you assign.

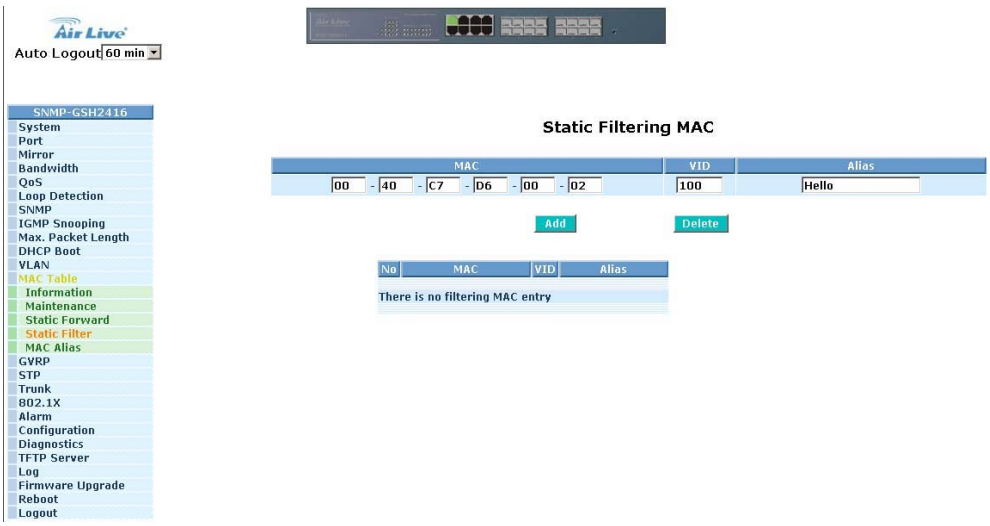


Fig. 3-41

Function name:

MAC Alias

Function description:

MAC Alias function is used to let you assign MAC address a plain English name. This will help you tell which MAC address belongs to which user in the illegal access report. At the initial time, it shows all pairs of the existed alias name and MAC address.

There are three MAC alias functions in this function folder, including MAC Alias Add, MAC Alias Edit and MAC Alias Delete. You can click **<Create/Edit>** button to add/modify a new or an existed alias name for a specified MAC address, or mark an existed entry to delete it. Alias name must be composed of A-Z, a-z and 0-9 only and has a maximal length of 15 characters.

Function name:

MAC Alias Create/Edit or Delete

Function description:

In the MAC Alias function, MAC Alias Add/Edit function is used to let you add or modify an association between MAC address and a plain English name. User can click **<Create/Edit>** button to add a new record with name.

As to MAC Alias Delete function is used to let you remove an alias name to a MAC address. You can select an existed MAC address or alias name to remove.

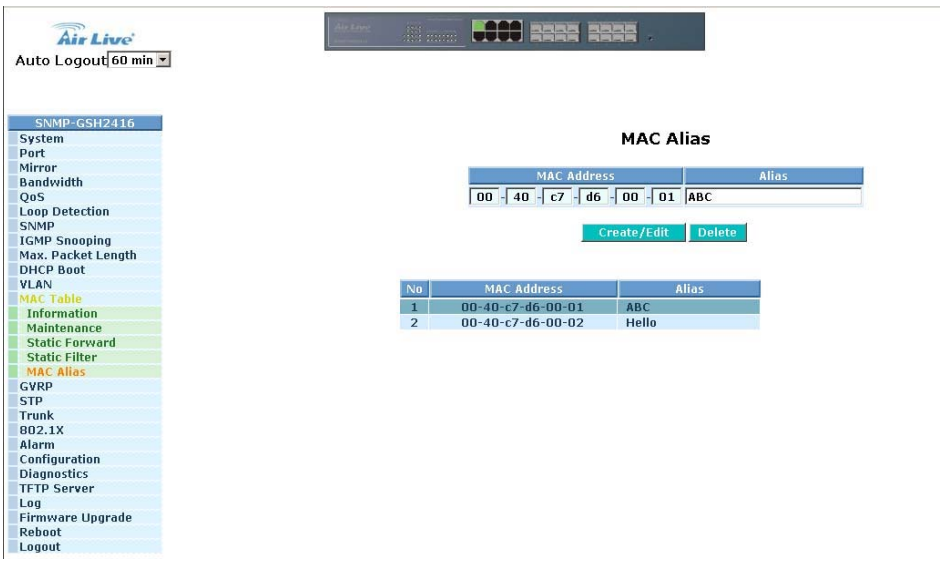


Fig. 3-42

Parameter description:

MAC Address:

It is a six-byte long Ethernet hardware address and usually expressed by hex and separated by hyphens. For example,

00 – 40 - C7 - D6 – 00 - 01

Alias:

MAC alias name you assign.

Note: If there are too many MAC addresses learned in the table, we recommend you inputting the MAC address and alias name directly.

3-12. GVRP Configuration

GVRP is an application based on Generic Attribute Registration Protocol (GARP), mainly used to automatically and dynamically maintain the group membership information of the VLANs. The GVRP offers the function providing the VLAN registration service through a GARP application. It makes use of GARP Information Declaration (GID) to maintain the ports associated with their attribute database and GARP Information Propagation (GIP) to communicate among switches and end stations. With GID information and GIP, GVRP state machine maintain the contents of Dynamic VLAN Registration Entries for each VLAN and propagate these information to other GVRP-aware devices to setup and update their knowledge database, the set of VLANs associated with currently active members, and through which ports these members can be reached.

In GVRP Configuration function folder, there are three functions supported, including GVRP Config, GVRP Counter and GVRP Group explained below.

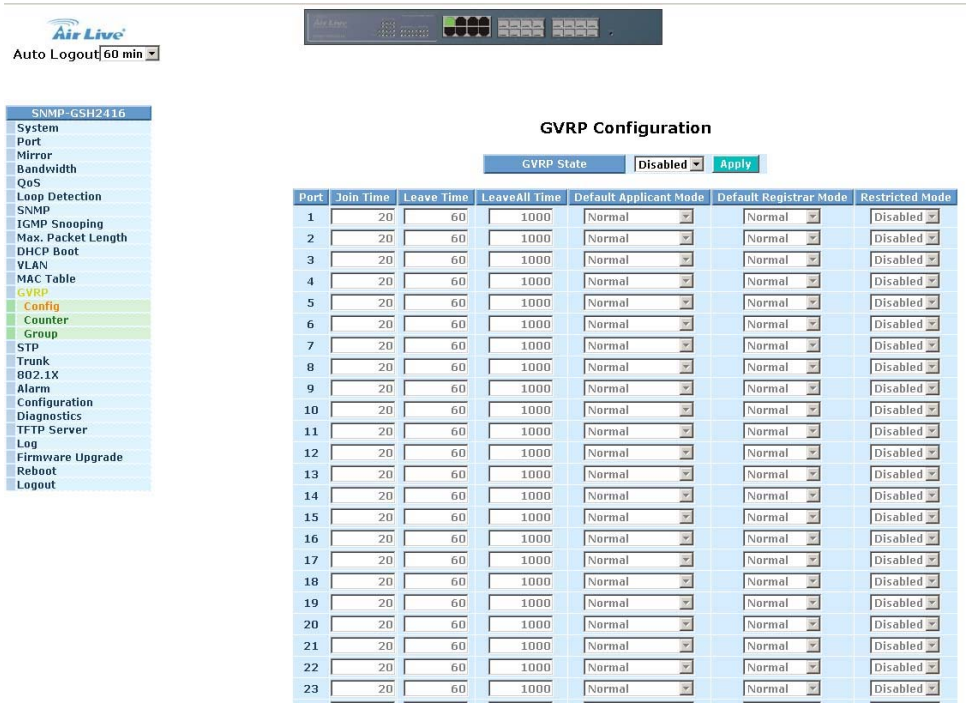


Fig. 3-43

Function name:

GVRP Config

Function description:

In the function of GVRP Config, it is used to configure each port's GVRP operation mode, in which there are seven parameters needed to be configured described below.

Parameter description:

GVRP State Setting:

This function is simply to let you enable or disable GVRP function. You can pull down the list and click the **<Downward>** arrow key to choose "Enable" or "Disable". Then, click the **<Apply>** button, the system will take effect immediately.

Join Time:

Used to declare the Join Time in unit of centisecond. Valid time range: 20 –100 centisecond, Default: 20 centisecond.

Leave Time:

Used to declare the Leave Time in unit of centisecond. Valid time range: 60 –300 centisecond, Default: 60 centisecond.

Leave All Time:

A time period for announcement that all registered device is going to be de-registered. If someone still issues a new join, then a registration will be kept in the switch. Valid range: 1000-5000 unit time, Default: 1000 unit time.

Default Applicant Mode:

The mode here means the type of participant. There are two modes, normal participant and non-participant, provided for the user's choice.

Normal:

It is Normal Participant. In this mode, the switch participates normally in GARP protocol exchanges. The default setting is Normal.

Non-Participant:

It is Non-Participant. In this mode, the switch does not send or reply any GARP messages. It just listens messages and reacts for the received GVRP BPDU.

Default Registrar Mode:

The mode here means the type of Registrar. There are three types of parameters for registrar administrative control value, normal registrar, fixed registrar and forbidden registrar, provided for the user's choice.

Normal:

It is Normal Registration. The Registrar responds normally to incoming GARP messages. The default setting is Normal.

Fixed:

It is Registration Fixed. The Registrar ignores all GARP messages, and all members remain in the registered (IN) state.

Forbidden:

It is Registration Forbidden. The Registrar ignores all GARP messages, and all members remain in the unregistered (EMPTY) state.

Restricted Mode:

This function is used to restrict dynamic VLAN be created when this port received GVRP PDU. There are two modes, disable and enable, provided for the user's choice.

Disabled:

In this mode, the switch dynamic VLAN will be created when this port received GVRP PDU. The default setting is Normal.

Enabled:

In this mode, the switch does not create dynamic VLAN when this port received GVRP PDU. Except received dynamic VLAN message of the GVRP PDU is an existed static VLAN in the switch, this port will be added into the static VLAN members dynamically.

Function name:

GVRP Counter

Function description:

All GVRP counters are mainly divided into Received and Transmitted two categories to let you monitor the GVRP actions. Actually, they are GARP packets.

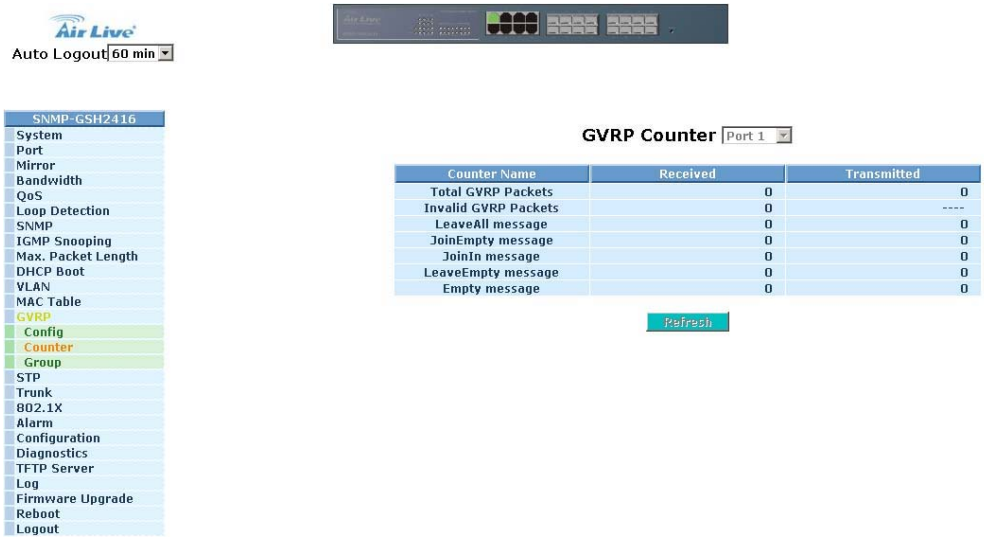


Fig. 3-44

Parameter description:

Received:

Total GVRP Packets:

Total GVRP BPDU is received by the GVRP application.

Invalid GVRP Packets:

Number of invalid GARP BPDU is received by the GARP application.

LeaveAll Message Packets:

Number of GARP BPDU with Leave All message is received by the GARP application.

JoinEmpty Message Packets:

Number of GARP BPDU with Join Empty message is received by the GARP application.

JoinIn Message Packets:

Number of GARP BPDU with Join In message is received by the GARP application.

LeaveEmpty Message Packets:

Number of GARP BPDU with Leave Empty message is received by the GARP application.

Empty Message Packets:

Number of GARP BPDU with Empty message is received by the GARP application.

Transmitted:

Total GVRP Packets:

Total GARP BPDU is transmitted by the GVRP application.

Invalid GVRP Packets:

Number of invalid GARP BPDU is transmitted by the GVRP application.

LeaveAll Message Packets:

Number of GARP BPDU with Leave All message is transmitted by the GARP application.

JoinEmpty Message Packets:

Number of GARP BPDU with Join Empty message is transmitted by the GARP application.

JoinIn Message Packets:

Number of GARP BPDU with Join In message is transmitted by the GARP application.

LeaveEmpty Message Packets:

Number of GARP BPDU with Leave Empty message is transmitted by the GARP application.

Empty Message Packets:

Number of GARP BPDU with Empty message is transmitted by the GARP application.

Function name:

GVRP Group Information

Function description:

To show the dynamic group member and their information.

Parameter description:

VID:

VLAN identifier. When GVRP group creates, each dynamic VLAN group owns its VID. Valid range is 1 ~ 4094.

Member Port:

Those are the members belonging to the same dynamic VLAN group.

Edit Administrative Control:

When you create GVRP group, you can use Administrative Control function to change Applicant Mode and Registrar Mode of GVRP group member.

Refresh:

Refresh function can help you to see current GVRP group status.

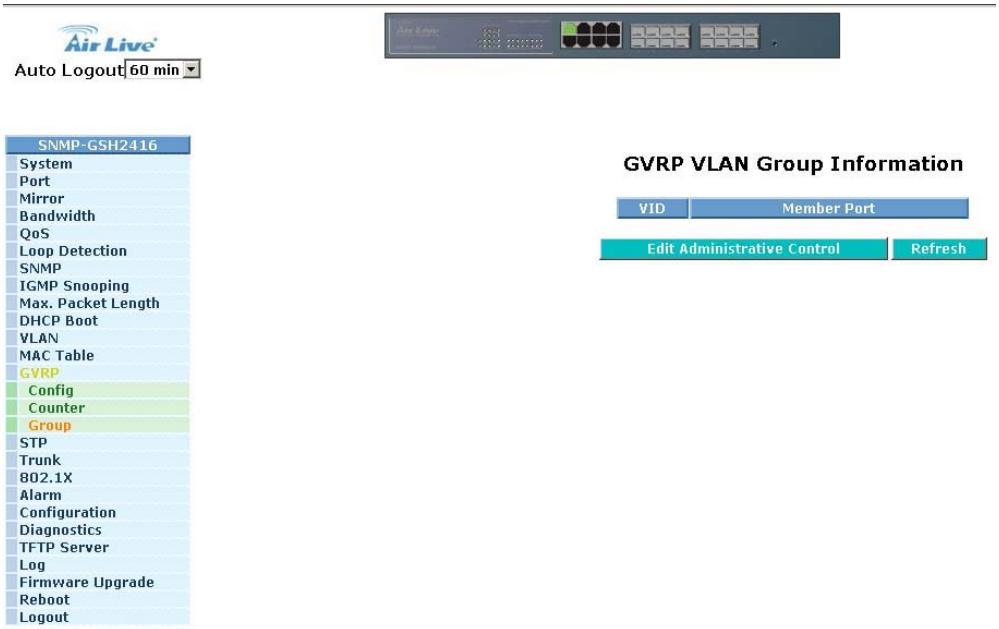


Fig. 3-45

3-13. STP Configuration

The Spanning Tree Protocol (STP) is a standardized method (IEEE 802.1D) for avoiding loops in switched networks. When STP is enabled, ensure that only one path is active between any two nodes on the network at a time. User can enable Spanning Tree Protocol on switch's web management and then set up other advanced items. We recommend that you enable STP on all switches to ensure a single active path on the network.

3-13-1. STP Status

Function name:

STP Status

Function description:

In the Spanning Tree Status, user can read 12 parameters to know STP current status. The 12 parameters' description is listed in the following table.

Parameter description:

STP State:

Show the current STP Enabled / Disabled status. Default is "Disabled".

Bridge ID:

Show switch's bridge ID which stands for the MAC address of this switch.

Bridge Priority:

Show this switch's current bridge priority setting. Default is 32768.

Designated Root:

Show root bridge ID of this network segment. If this switch is a root bridge, the "Designated Root" will show this switch's bridge ID.

Designated Priority:

Show the current root bridge priority.

Root Port:

Show port number connected to root bridge with the lowest path cost.

Root Path Cost:

Show the path cost between the root port and the designated port of the root bridge.

Current Max. Age:

Show the current root bridge maximum age time. Maximum age time is used to monitor if STP topology needs to change. When a bridge does not receive a hello message from root bridge until the maximum age time is counted down to 0, the bridge will treat the root bridge malfunctioned and issue a Topology Change Notification (TCN) BPDU to all other bridges.

All bridges in the LAN will re-learn and determine which the root bridge is. Maximum Age time is assigned by root bridge in unit of seconds. Default is 20 seconds.

Current Forward Delay:

Show the current root bridge forward delay time. The value of Forward Delay time is set by root. The Forward Delay time is defined as the time spent from Listening state moved to Learning state or from Learning state moved to Forwarding state of a port in bridge.

Hello Time:

Show the current hello time of the root bridge. Hello time is a time interval specified by root bridge, used to request all other bridges periodically sending hello message every “hello time” seconds to the bridge attached to its designated port.

STP Topology Change Count:

STP Topology Change Count expresses the time spent in unit of seconds since the beginning of the Spanning Tree Topology Change to the end of the STP convergence. Once the STP change is converged, the Topology Change count will be reset to 0. The figures showing in the screen may not be the exact time it spent but very close to, because the time is eclipsing.

Time Since Last Topology Change:

Time Since Last Topology Change is the accumulated time in unit of seconds the STP has been since the last STP Topology Change was made. When Topology Change is initiated again, this counter will be reset to 0. And it will also count again once STP topology Change is completed.

Fig. 3-46

3-13-2. STP Configuration

The STP, Spanning Tree Protocol, actually includes RSTP. In the Spanning Tree Configuration, there are six parameters open for the user to configure as user's idea. Each parameter description is listed below.

Function name:

STP Configuration

Function description:

User can set the following Spanning Tree parameters to control STP function enable/disable, select mode RSTP/STP and affect STP state machine behavior to send BPDU in this switch. The default setting of Spanning Tree Protocol is "Disable".

Parameter description:

Spanning Tree Protocol:

Set 802.1W Rapid STP function Enable / Disable. Default is "Disable"

Bridge Priority:

The lower the bridge priority is, the higher priority it has. Usually, the bridge with the highest bridge priority is the root. If you want to have the SNMP-GSH2416 as root bridge, you can set this value lower than that of bridge in the LAN. The valid value is 0 ~ 61440. The default is 32768.

Hello Time:

Hello Time is used to determine the periodic time to send normal BPDU from designated ports among bridges. It decides how long a bridge should send this message to other bridge to tell I am alive. When the SNMP-GSH2416 is the root bridge of the LAN, for example, all other bridges will use the hello time assigned by this switch to communicate with each other. The valid value is 1 ~ 10 in unit of second.

Default is 2 seconds.

Max. Age:

When the SNMP-GSH2416 is the root bridge, the whole LAN will apply this figure set by this switch as their maximum age time. When a bridge received a BPDU originated from the root bridge and if the message age conveyed in the BPDU exceeds the Max. Age of the root bridge, the bridge will treat the root bridge malfunctioned and issue a Topology Change Notification (TCN) BPDU to all other bridges. All bridges in the LAN will re-calculate and determine who the root bridge is. The valid value of Max. Age is 6 ~ 40 seconds. Default is 20 seconds.

Forward Delay:

You can set the root bridge forward delay time. This figure is set by root bridge only. The forward delay time is defined as the time spent from Listening state moved to Learning state and also from Learning state moved to Forwarding state of a port in bridge. The forward delay time contains two states, Listening state to Learning state and Learning state to Forwarding state. It assumes that forward delay time is 15 seconds, then total forward delay time will be 30 seconds. This has much to do with the STP convergent time which will be more than 30 seconds because some other factors.

The valid value is 4 ~ 30 seconds, default is 15 seconds.

Force Version:

Two options are offered for the user's choosing STP algorithm. One is RSTP and the other is STP. If STP is chosen, RSTP will run as a legacy STP. The switch supports RSTP (802.1w) which is backward compatible with STP (802.1d).

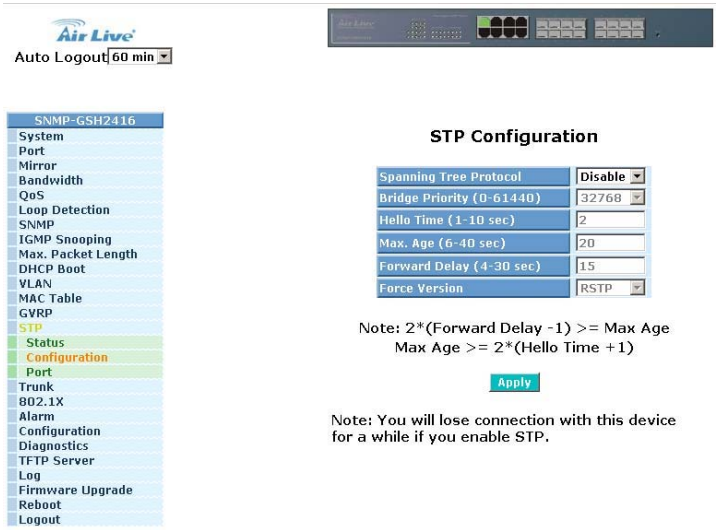


Fig. 3-47

3-13-3. STP Port Configuration

Function name:

STP Port Setting

Function description:

In the STP Port Setting, one item selection and five parameters settings are offered for user's setup. User can disable and enable each port by selecting each Port Status item. User also can set "Path Cost" and "Priority" of each port by filling in the desired value and set "Admin Edge Port" and "Admin Point To Point" by selecting the desired item.

Parameter description:

Port Status:

It displays the current state of a port. We cannot manually set it because it displays the status only. There are three possible states. (according to 802.1w specification)

- DISCARDING state indicates that this port can neither forward packets nor contribute learning knowledge.

Notice: Three other states (Disable state, BLOCKING state and LISTENING state) defined in the 802.1d specification are now all represented as DISCARDING state.

- LEARNING state indicates this port can now contribute its learning knowledge but cannot forward packets still.

- FORWARDING state indicates this port can both contribute its learning knowledge and forward packets normally.

Path Cost Status:

It is the contribution value of the path through this port to Root Bridge. STP algorithm determines a best path to Root Bridge by calculating the sum of path cost contributed by all ports on this path. A port with a smaller path cost value would become the Root Port more possibly.

Configured Path Cost:

The range is 0 – 200,000,000. In the switch, if path cost is set to be zero, the STP will get the recommended value resulted from auto-negotiation of the link accordingly and display this value in the field of Path Cost Status. Otherwise, it may show the value that the administrator set up in Configured Path Cost and Path Cost Status.

802.1w RSTP recommended value: (Valid range: 1 – 200,000,000)

10 Mbps : 2,000,000

100 Mbps : 200,000

1 Gbps : 20,000

Default: 0

Priority:

Priority here means Port Priority. Port Priority and Port Number are mixed to form the Port ID. Port IDs are often compared in order to determine which port of a bridge would become the Root Port. The range is 0 – 240.

Default is 128.

Admin Edge Port:

If user selects “Yes”, this port will be an edge port. An Edge Port is a port connected to a device that knows nothing about STP or RSTP. Usually, the connected device is an end station. Edge Ports will immediately transit to forwarding state and skip the listening and learning state because the edge ports cannot create bridging loops in the network. This will expedite the convergence. When the link on the edge port toggles, the STP topology keeps unchanged. Unlike the designate port or root port though, an edge port will transit to a normal spanning-tree port immediately if it receives a BPDU.

Default: No

Admin Point To Point:

We say a port is a point-to-point link, from RSTP’s view, if it is in full-duplex mode but is shared link if it is in half-duplex mode. RSTP fast convergence can only happen on point-to-point links and on edge ports. This can expedite the convergence because this will have the port fast transited to forwarding state.

There are three parameters, Auto, True and False, used to configure the type of the point-to-point link. If configure this parameter to be Auto, it means RSTP will use the duplex mode resulted from the auto-negotiation. In today’s switched networks, most links are running in full-duplex mode. For sure, the result may be half-duplex, in this case, the port will not fast transit to Forwarding state. If it is set as True, the port is treated as point-to-point link by RSTP and unconditionally transited to Forwarding state. If it is set as False, fast transition to Forwarding state will not happen on this port.

Default: Auto

M Check:

Migration Check. It forces the port sending out an RSTP BPDU instead of a legacy STP BPDU at the next transmission. The only benefit of this operation is to make the port quickly get back to act as an RSTP port. Click **<M Check>** button to send a RSTP BPDU from the port you specified.

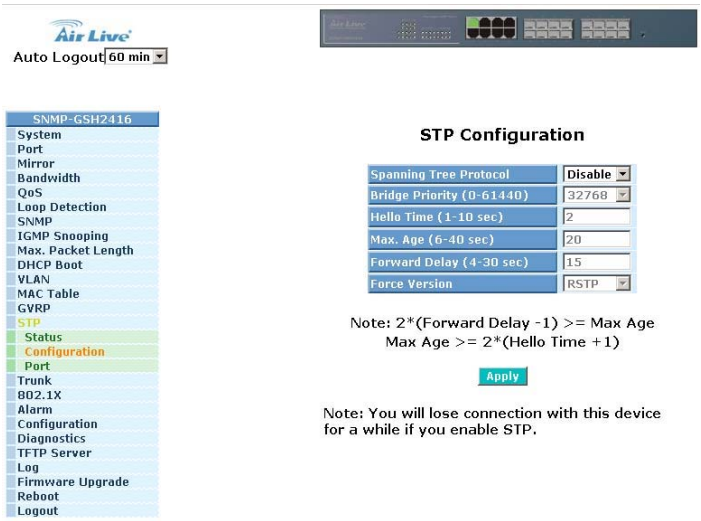


Fig. 3-48

3-14. Trunking Configuration

The Port Trunking Configuration is used to configure the settings of Link Aggregation. You can bundle more than one port with the same speed, full duplex and the same MAC to be a single logical port, thus the logical port aggregates the bandwidth of these ports. This means you can apply your current Ethernet equipments to build the bandwidth aggregation. For example, if there are three Fast Ethernet ports aggregated in a logical port, then this logical port has bandwidth three times as high as a single Fast Ethernet port has.

The switch supports two kinds of port trunking methods:

LACP:

Ports using Link Aggregation Control Protocol (according to IEEE 802.3ad specification) as their trunking method can choose their unique LACP GroupID (1~8) to form a logic “trunked port”. The benefit of using LACP is that a port makes an agreement with its peer port before it becomes a ready member of a “trunk group” (also called aggregator). LACP is safer than the other trunking method - static trunk.

The switch LACP does not support the followings:

- Link Aggregation across switches
- Aggregation with non-IEEE 802.3 MAC link
- Operating in half-duplex mode
- Aggregate the ports with different data rates

Static Trunk:

Ports using Static Trunk as their trunk method can choose their unique Static GroupID (also 1~8, this Static groupID can be the same with another LACP groupID) to form a logic “trunked port”. The benefit of using Static Trunk method is that a port can immediately become a member of a trunk group without any handshaking with its peer port. This is also a disadvantage because the peer ports of your static trunk group may not know that they should be aggregate together to form a “logic trunked port”. Using Static Trunk on both end of a link is strongly recommended. Please also note that low speed links will stay in “not ready” state when using static trunk to aggregate with high speed links.

As to system restrictions about the port aggregation function on the switch, In the management point of view, the switch supports maximum 8 trunk groups for LACP and additional 8 trunk groups for Static Trunk. But in the system capability view, only 8 “real trunked” groups are supported. An LACP trunk group with more than one ready member-ports is a “real trunked” group. An LACP trunk group with only one or less than one ready member-ports is not a “real trunked” group. Any Static trunk group is a “real trunked” group.

Per Trunking Group supports a maximum of 12 ready member-ports. Please note that some decisions will automatically be made by the system while you are configuring your trunking ports. Some configuration examples are listed below:

a) 12 ports have already used Static Trunk Group ID 1, the 13th port willing to use the same Static Trunk Group ID will be automatically set to use the “None” trunking method and its Group ID will turn to 0. This means the port won’t aggregate with other ports.

b) 14 ports all use LACP Trunk Group ID 1 at most 12 ports can aggregate together and transit into the ready state.

c) A port using the “None“ trunking method or Group ID 0 will be automatically set to use the “None” trunking method with Group ID 0.

Function name:

Port Setting/Status

Function description:

Port setting/status is used to configure the trunk property of each and every port in the switch system.

Parameter description:

Method:

This determines the method a port uses to aggregate with other ports.

None:

A port does not want to aggregate with any other port should choose this default setting.

LACP:

A port use LACP as its trunk method to get aggregated with other ports also using LACP.

Static:

A port use Static Trunk as its trunk method to get aggregated with other ports also using Static Trunk.

Group:

Ports choosing the same trunking method other than “None” must be assigned a unique Group number (i.e. Group ID, valid value is from 1 to 8) in order to declare that they wish to aggregate with each other.

Active LACP:

This field is only referenced when a port’s trunking method is LACP.

Active:

An Active LACP port begins to send LACPDU to its link partner right after the LACP protocol entity started to take control of this port.

Passive:

A Passive LACP port will not actively send LACPDU out before it receives an LACPDU from its link partner.

Aggtr:

Aggtr is an abbreviation of “aggregator”. Every port is also an aggregator, and its own aggregator ID is the same as its own Port No. We can regard an aggregator as a representative of a trunking group. Ports with same Group ID and using same trunking method will have the opportunity to aggregate to a particular aggregator port. This aggregator port is usually the port with the smallest Port No. within the trunking group.

Status:

This field represents the trunking status of a port which uses a trunking method other than “None”. It also represents the management link status of a port which uses the “None” trunking method. “---“ means “not ready”

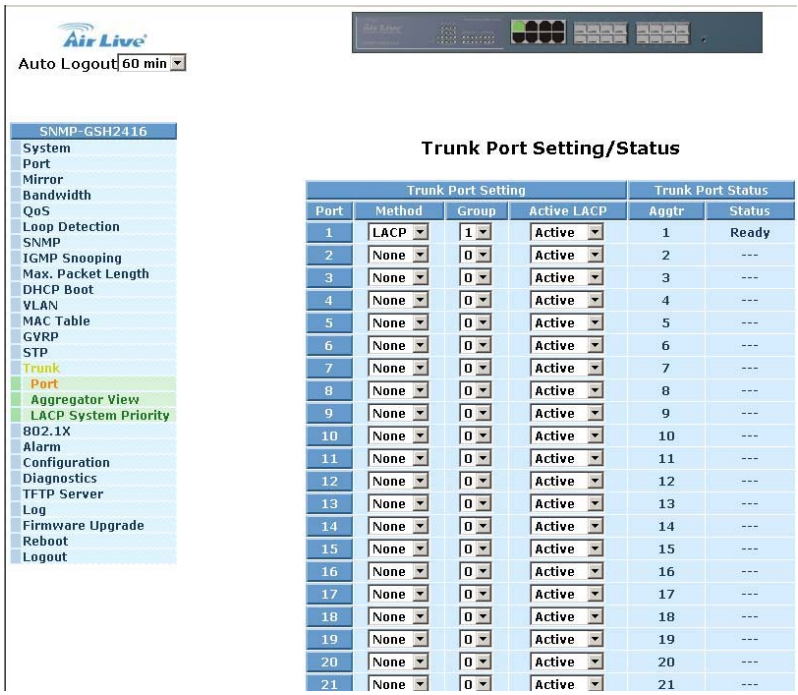


Fig.3-49

Function name:

Aggregator View

Function description:

To display the current port trunking information from the aggregator point of view.

Parameter description:

Aggregator:

It shows the aggregator ID (from 1 to 24) of every port. In fact, every port is also an aggregator, and its own aggregator ID is the same as its own Port No..

Method:

Show the method a port uses to aggregate with other ports.

Member Ports:

Show all member ports of an aggregator (port).

Ready Ports:

Show only the ready member ports within an aggregator (port).

Fig.3-50

Function name:

LACP Detail (LACP Aggregator Detailed Information)

Function description:

Show the detailed information of the LACP trunking group.

Parameter description:

Actor:

The switch you are watching on.

Partner:

The peer system from this aggregator's view.

System Priority:

Show the System Priority part of a system ID.

MAC Address:

Show the MAC Address part of a system ID.

Port:

Show the port number part of an LACP port ID.

Key:

Show the key value of the aggregator. The key value is determined by the LACP protocol entity and can't be set through management.

Trunk Status:

Show the trunk status of a single member port."---" means "not ready"

Fig. 4-51

Function name:

LACP System Priority

Function description:

It is used to set the priority part of the LACP system ID. LACP will only aggregate together the ports whose peer link partners are all on a single system. Each system supports LACP will be assigned a globally unique System Identifier for this purpose. A system ID is a 64-bit field comprising a 48-bit MAC Address and 16-bit priority value. The System Priority can be set by the user. Its range is from 1 to 65535. Default: 32768

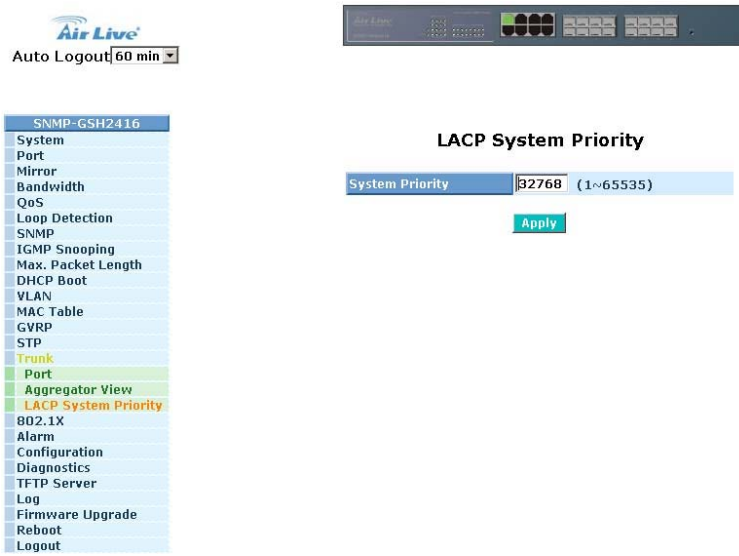


Fig.3-52

3-15. 802.1X Configuration

802.1X port-based network access control provides a method to restrict users to access network resources via authenticating user's information. This restricts users from gaining access to the network resources through a 802.1X-enabled port without authentication. If a user wishes to touch the network through a port under 802.1X control, he (she) must firstly input his (her) account name for authentication and waits for gaining authorization before sending or receiving any packets from a 802.1X-enabled port.

Before the devices or end stations can access the network resources through the ports under 802.1X control, the devices or end stations connected to a controlled port send the authentication request to the authenticator, the authenticator pass the request to the authentication server to authenticate and verify, and the server tell the authenticator if the request get the grant of authorization for the ports.

According to IEEE802.1X, there are three components implemented. They are Authenticator, Supplicant and Authentication server shown in Fig. 3-53.

Supplicant:

It is an entity being authenticated by an authenticator. It is used to communicate with the Authenticator PAE (Port Access Entity) by exchanging the authentication message when the Authenticator PAE request to it.

Authenticator:

An entity facilitates the authentication of the supplicant entity. It controls the state of the port, authorized or unauthorized, according to the result of authentication message exchanged between it and a supplicant PAE. The authenticator may request the supplicant to re-authenticate itself at a configured time period. Once start re-authenticating the supplicant, the controlled port keeps in the authorized state until re-authentication fails.

A port acting as an authenticator is thought to be two logical ports, a controlled port and an uncontrolled port. A controlled port can only pass the packets when the authenticator PAE is authorized, and otherwise, an uncontrolled port will unconditionally pass the packets with PAE group MAC address, which has the value of 01-80-c2-00-00-03 and will not be forwarded by MAC bridge, at any time.

Authentication server:

A device provides authentication service, through EAP, to an authenticator by using authentication credentials supplied by the supplicant to determine if the supplicant is authorized to access the network resource.

The overview of operation flow for the Fig. 3-53 is quite simple. When Supplicant PAE issues a request to Authenticator PAE, Authenticator and Supplicant exchanges authentication message. Then, Authenticator passes the request to RADIUS server to verify. Finally, RADIUS server replies if the request is granted or denied.

While in the authentication process, the message packets, encapsulated by Extensible Authentication Protocol over LAN (EAPOL), are exchanged between an authenticator PAE and a supplicant PAE. The Authenticator exchanges the message to authentication server using EAP encapsulation. Before successfully authenticating, the supplicant can only touch the authenticator to perform authentication message exchange or access the network from the uncontrolled port.

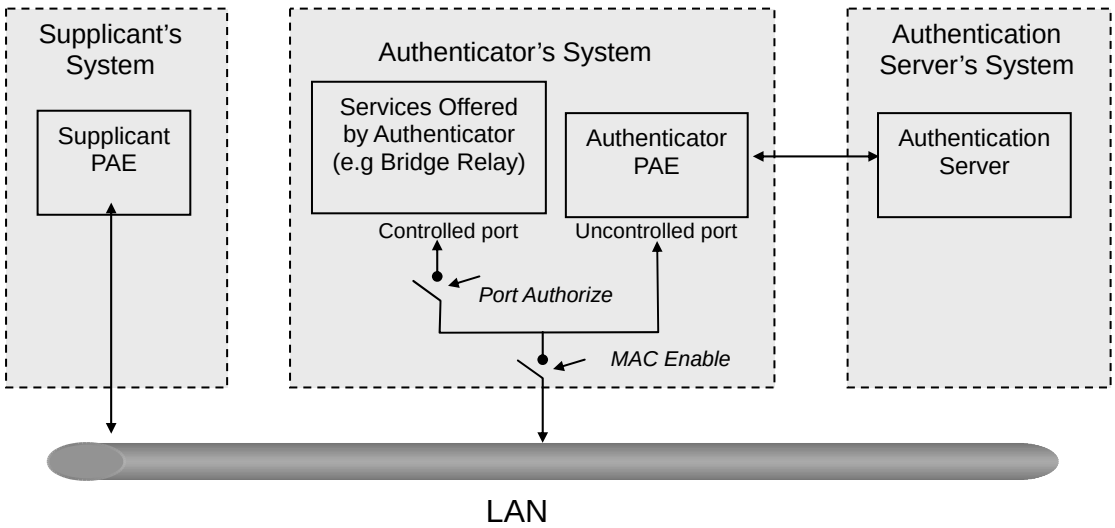
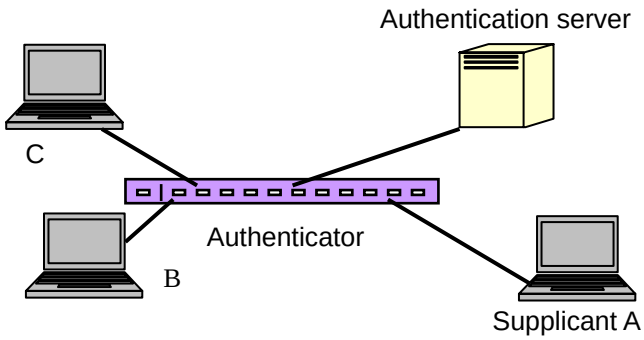


Fig. 3-53

In the Fig. 3-54, this is the typical configuration, a single supplicant, an authenticator and an authentication server. B and C is in the internal network, D is Authentication server running RADIUS, switch at the central location acts Authenticator connecting to PC A and A is a PC outside the controlled port, running Supplicant PAE. In this case, PC A wants to access the services on device B and C, first, it must exchange the authentication message with the authenticator on the port it connected via EAPOL packet. The authenticator transfers the supplicant's credentials to Authentication server for verification. If success, the authentication server will notice the authenticator the grant. PC A, then, is allowed to access B and C via the switch. If there are two switches directly connected together instead of single one, for the link connecting two switches, it may have to act two port roles at the end of the link: authenticator and supplicant, because the traffic is bi-directional.

Fig. 3-54



The Fig. 3-55 shows the procedure of 802.1X authentication. There are steps for the login based on 802.1X port access control management. The protocol used in the right side is EAPOL and the left side is EAP.

1. At the initial stage, the supplicant A is unauthenticated and a port on switch acting as an authenticator is in unauthorized state. So the access is blocked in this stage.

2. Initiating a session. Either authenticator or supplicant can initiate the message exchange. If supplicant initiates the process, it sends EAPOL-start packet to the authenticator PAE and authenticator will immediately respond EAP-Request/Identity packet.

3. The authenticator always periodically sends EAP-Request/Identity to the supplicant for requesting the identity it wants to be authenticated.

4. If the authenticator doesn't send EAP-Request/Identity, the supplicant will initiate EAPOL-Start the process by sending to the authenticator.

5. And next, the Supplicant replies an EAP-Response/Identity to the authenticator. The authenticator will embed the user ID into Radius-Access-Request command and send it to the authentication server for confirming its identity.

6. After receiving the Radius-Access-Request, the authentication server sends Radius-Access-Challenge to the supplicant for asking for inputting user password via the authenticator PAE.

7. The supplicant will convert user password into the credential information, perhaps, in MD5 format and replies an EAP-Response with this credential information as well as the specified authentication algorithm (MD5 or OTP) to Authentication server via the authenticator PAE. As per the value of the type field in message PDU, the authentication server knows which algorithm should be applied to authenticate the credential information, EAP-MD5 (Message Digest 5) or EAP-OTP (One Time Password) or other else algorithm.

8. If user ID and password is correct, the authentication server will send a Radius-Access-Accept to the authenticator. If not correct, the authentication server will send a Radius-Access-Reject.

9. When the authenticator PAE receives a Radius-Access-Accept, it will send an EAP-Success to the supplicant. At this time, the supplicant is authorized and the port connected to the supplicant and under 802.1X control is in the authorized state. The supplicant and other devices connected to this port can access the network. If the authenticator receives a Radius-Access-Reject, it will send an EAP-Failure to the supplicant. This means the supplicant is failed to authenticate. The port it connected is in the unauthorized state, the supplicant and the devices connected to this port won't be allowed to access the network.

10. When the supplicant issue an EAP-Logoff message to Authentication server, the port you are using is set to be unauthorized.

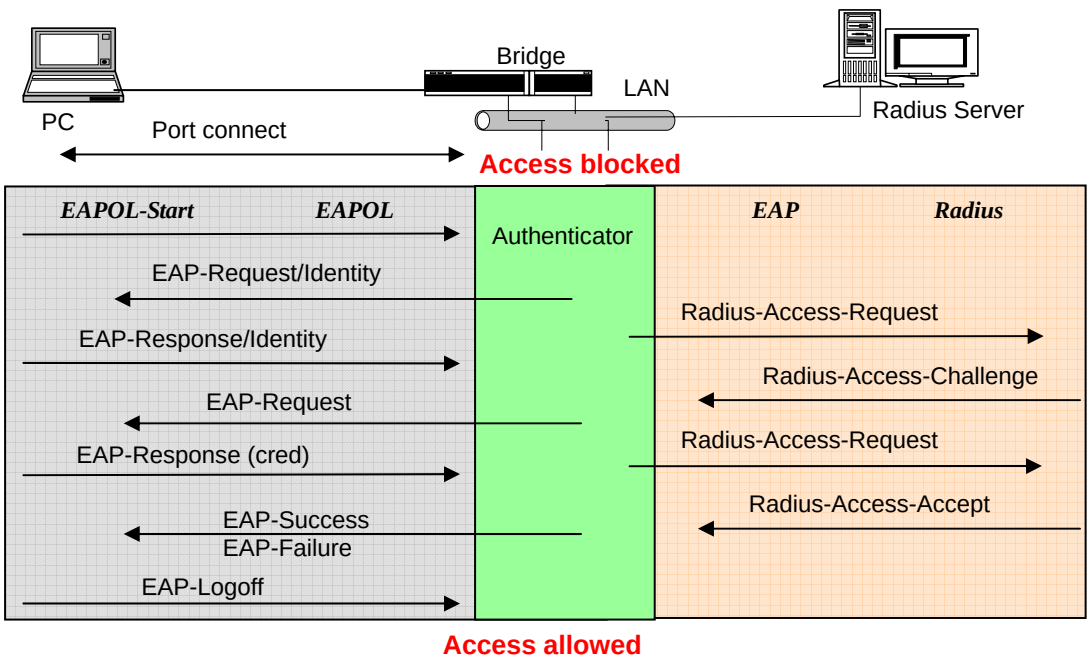


Fig. 3-55

Only MultiHost 802.1X is the type of authentication supported in the switch. In this mode, for the devices connected to this port, once a supplicant is authorized, the devices connected to this port can access the network resource through this port.

802.1X Port-based Network Access Control function supported by the switch is little bit complex, for it just support basic Multihost mode, which can distinguish the device's MAC address and its VID. The following table is the summary of the combination of the authentication status and the port status versus the status of port mode, set in 802.1X Port mode, port control state, set in 802.1X port setting. Here Entry Authorized means MAC entry is authorized.

Port Mode	Port Control	Authentication	Port Status
Disable	Don't Care	Don't Care	Port Uncontrolled
Multihost	Auto	Successful	Port Authorized
Multihost	Auto	Failure	Port Unauthorized
Multihost	ForceUnauthorized	Don't Care	Port Unauthorized
Multihost	ForceAuthorized	Don't Care	Port Authorized

Table 3-3

Function name:

802.1X State Setting

Function description:

This function is used to configure the global parameters for RADIUS authentication in 802.1X port security application.

Parameter description:

Radius Server:

RADIUS server IP address for authentication.

Default: 192.168.1.1

Port Number:

The port number to communicate with RADIUS server for the authentication service. The valid value ranges 1-65535.

Default port number is 1812.

Secret Key:

The secret key between authentication server and authenticator. It is a string with the length 1 – 31 characters. The character string may contain upper case, lower case and 0-9. It is character sense. It is not allowed for putting a blank between any two characters.

Default: Radius

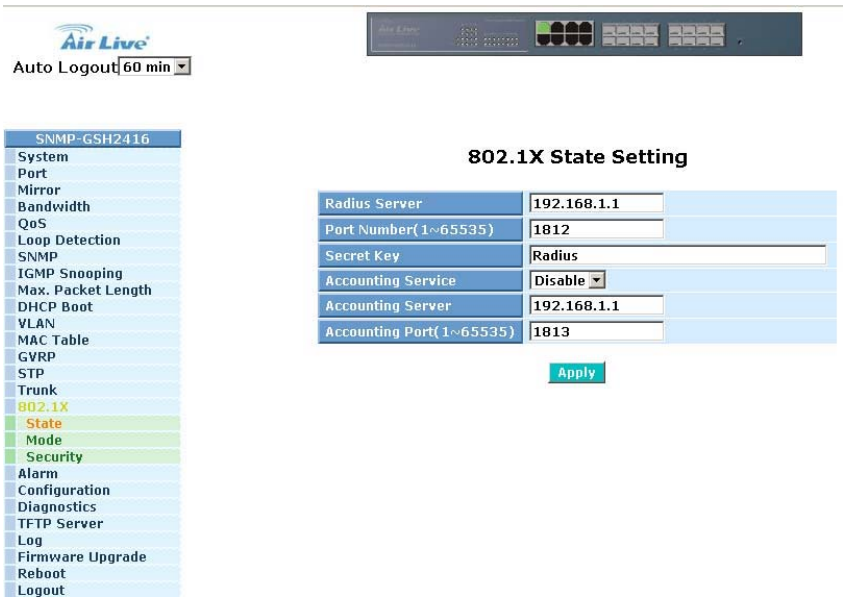


Fig. 3-56

Function name:

802.1X Mode Setting

Function description:

Set the operation mode of 802.1X for each port. In this device, it supports only Multi-host operation mode.

Parameter description:

Port Number:

Indicate which port is selected to configure the 802.1X operation mode.

802.1X Mode:

802.1X operation mode. There are two options, including Disable and Multi-host mode. Default is Disable.

- Disable

It will have the chosen port acting as a plain port, that is no 802.1X port access control works on the port.

- 802.1X with Multi-host

In Multi-host mode, for the devices connected to this port, once a supplicant is authorized, the devices connected to this port can access the network resource through this port.

Fig. 3-57

Function name:

Port Security Management

Function description:

Shows each port status. In Multihost mode, it shows the port number and its status, authorized or unauthorized.

Parameter description:

Disable Mode:

When selecting Disable mode for a port in the function 802.1X Port Mode Configuration, the port is in the uncontrolled port state and does not apply 802.1X authenticator on it. Any node attached on this port can access the network without the admittance of 802.1X authenticator. The Port Status will show the following screen.

Port Number:

The port number to be chosen to show its 802.1X Port Status. The valid number is Port 1 – 24.

Port Status:

The current 802.1X status of the port. In Disable mode, this field is Disabled.

802.1X with Multihost mode:

When selecting 802.1X with Multihost mode for a port in the function 802.1X Port Mode Configuration, Devices can access the network through this port once the authenticator is authorized. The Port Status will show the following screen. If the port is granted to access the network, the port status is authorized, otherwise, unauthorized.

Fig. 3-58

Function name:

Param. Setting

Function description:

This function is used to configure the parameters for each port in 802.1X port security application. Refer to the following parameters description for details.

Parameter description:

Port:

It is the port number to be selected for configuring its associated 802.1X parameters which are Port control, reAuthMax, txPeriod, Quiet Period, reAuthEnabled, reAuthPeriod, max. Request, suppTimeout, serverTimeout and Controlled direction.

Port Control:

This is used to set the operation mode of authorization. There are three type of operation mode supported, ForceUnauthorized, ForceAuthorized, Auto.

- ForceUnauthorized:

  The controlled port is forced to hold in the unauthorized state.

- ForceAuthorized:

  The controlled port is forced to hold in the authorized state.

- Auto:

  The controlled port is set to be in authorized state or unauthorized state depends on the result of the authentication exchange between the authentication server and the supplicant.

  Default: Auto

reAuthMax(1-10):

The number of authentication attempt that is permitted before the port becomes unauthorized.

Default: 2

txPeriod(1-65535 s):

A time period to transmitted EAPOL PDU between the authenticator and the supplicant.

Default: 30

Quiet Period(0-65535 s):

A period of time during which we will not attempt to access the supplicant.

Deafult: 60 seconds

reAuthEnabled:

Choose whether regular authentication will take place in this port.

Default: ON

reAuthPeriod(1-65535 s):

A non-zero number seconds between the periodic re-authentication of the supplicant.

Default: 3600

max. Request(1-10):

The maximum of number times that the authenticator will retransmit an EAP Request to the supplicant before it times out the authentication session. The valid range: 1 – 10.

Default: 2 times

suppTimeout(1-65535 s):

A timeout condition in the exchange between the authenticator and the supplicant. The valid range: 1 –65535.

Default: 30 seconds.

serverTimeout(1-65535 s):

A timeout condition in the exchange between the authenticator and the authentication server. The valid range: 1 –65535.

Default: 30 seconds

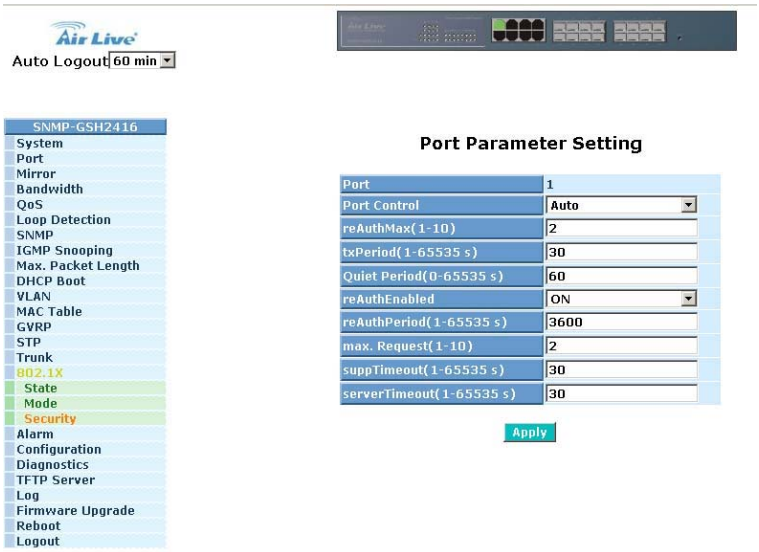
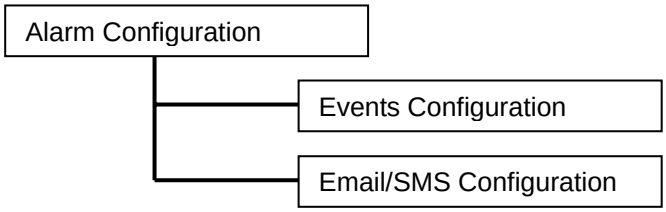


Fig. 3-59

3-16. Alarm Configuration



Function name:

Events Configuration

Function description:

The Trap Events Configuration function is used to enable the switch to send out the trap information while pre-defined trap events occurred. The switch offers 23 different trap events to users for switch management. The trap information can be sent out in three ways, including email, mobile phone SMS (short message system) and trap. The message will be sent while users tick (☑) the trap event individually on the web page shown as below.

Parameter description:

Trap: Cold Start, Warm Start, Link Down, Link Up, Authentication Failure, User login, User logout

STP: STP Topology Changed, STP Disabled, STP Enabled

LACP: LACP Disabled, LACP Enabled, LACP Member Added, LACP Port Failure

GVRP: GVRP Disabled, GVRP Enabled

VLAN: VLAN Disabled, Port-based VLAN Enabled, Tag-based VLAN Enabled, Metro-mode Vlan Enabled, Double-tag Vlan Enabled

Module Swap: Module Inserted, Module Removed

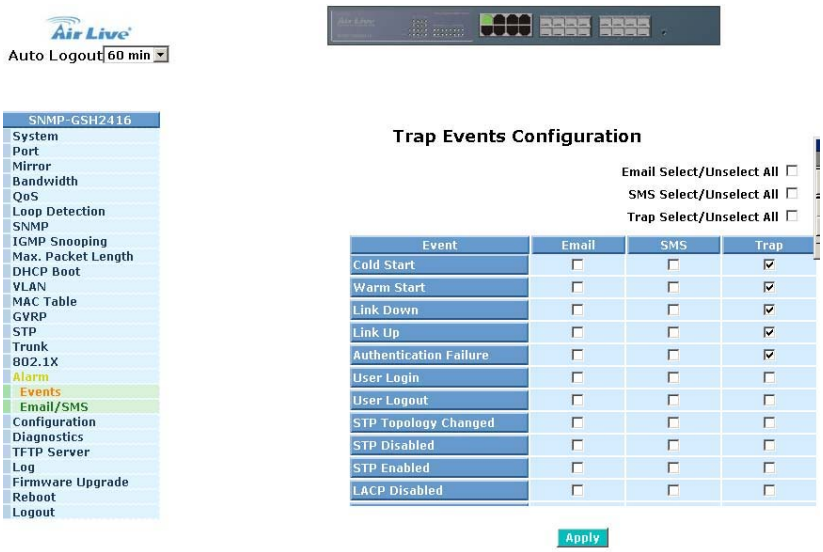


Fig. 3-60

Function name:

Email/SMS Configuration

Function description:

Alarm configuration is used to configure the persons who should receive the alarm message via either email or SMS, or both. It depends on your settings. An email address or a mobile phone number has to be set in the web page of alarm configuration (See Fig. 3-61). Then, user can read the trap information from the email or the mobile phone. This function provides 6 email addresses and 6 mobile phone numbers at most. The 23 different trap events will be sent out to SNMP Manager when trap event occurs. After ticking trap events, you can fill in your desired email addresses and mobile phone numbers. Then, please click **<Apply>** button to complete the alarm configuration. It will take effect in a few seconds.

Note: SMS may not work in your mobile phone system. It is customized for different systems.

Parameter description:

Email:

Mail Server: the IP address of the server transferring your email.

Username: your username on the mail server.

Password: your password on the mail server.

Email Address 1 – 6: email address that would like to receive the alarm message.

SMS:

SMS Server: the IP address of the server transferring your SMS.

Username: your username in ISP.

Password: your username in ISP.

Mobile Phone 1-6: the mobile phone number that would like to receive the alarm message.

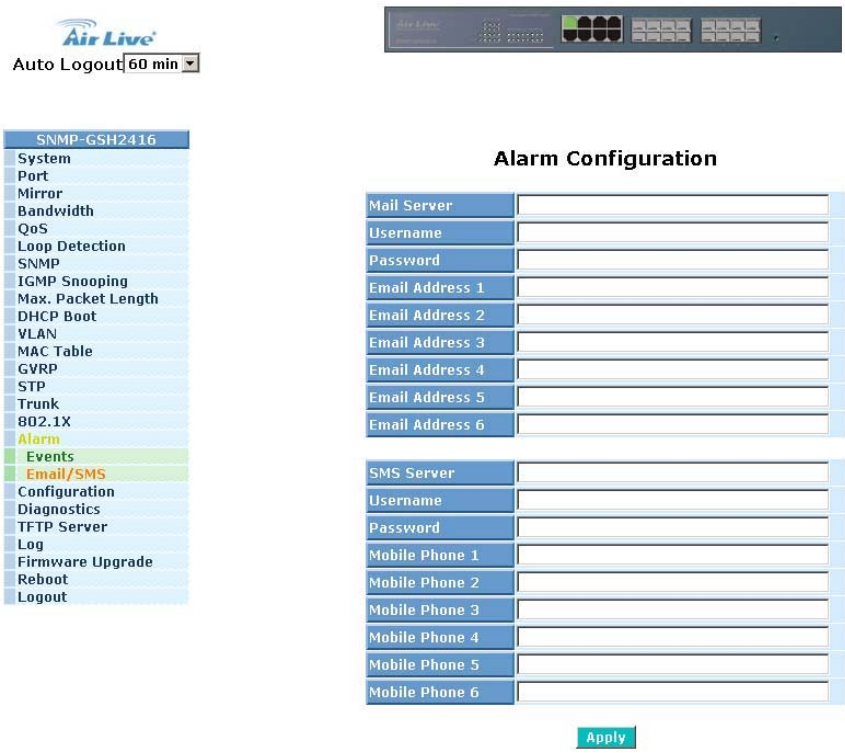


Fig. 3-61

3-17. Configuration

The switch supports three copies of configuration, including the default configuration, working configuration and user configuration for your configuration management. All of them are listed and described below respectively.

▪ **Default Configuration:**

This is the ex-factory setting and cannot be altered. In Web UI, two restore default functions are offered for the user to restore to the default setting of the switch. One is the function of “Restore Default Configuration included default IP address”, the IP address will restore to default “192.168.1.1” as you use it. The other is the function of “Restore Default Configuration without changing current IP address”, the IP address will keep the same one that you had saved before by performing this function.

▪ **Working Configuration:**

It is the configuration you are using currently and can be changed any time. The configurations you are using are saved into this configuration file. This is updated each time as you press **<Apply>** button.

▪ **User Configuration:**

It is the configuration file for the specified or backup purposes and can be updated while having confirmed the configuration. You can retrieve it by performing Restore User Configuration.

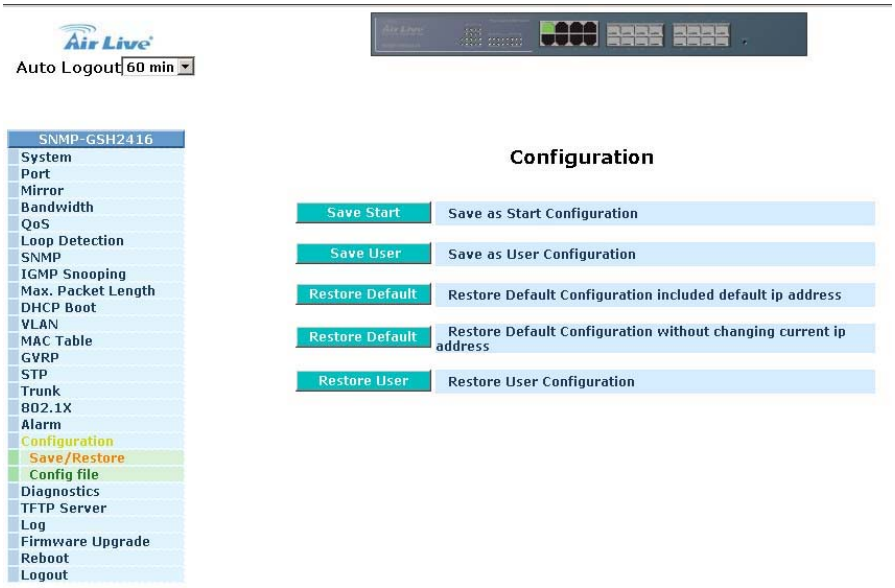


Fig. 3-62

3-17-1. Save/Restore

Function name:

Save As Start Configuration

Function description:

Save the current configuration as a start configuration file in flash memory.

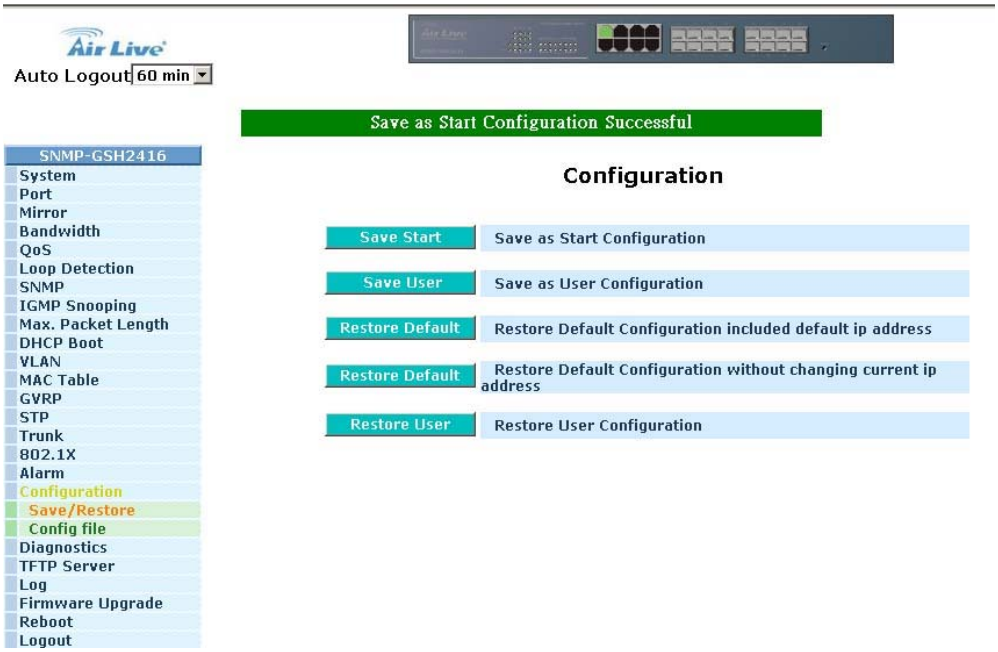


Fig. 3-63

Function name:

Save As User Configuration

Function description:

Save the current configuration as a user configuration file in flash memory.

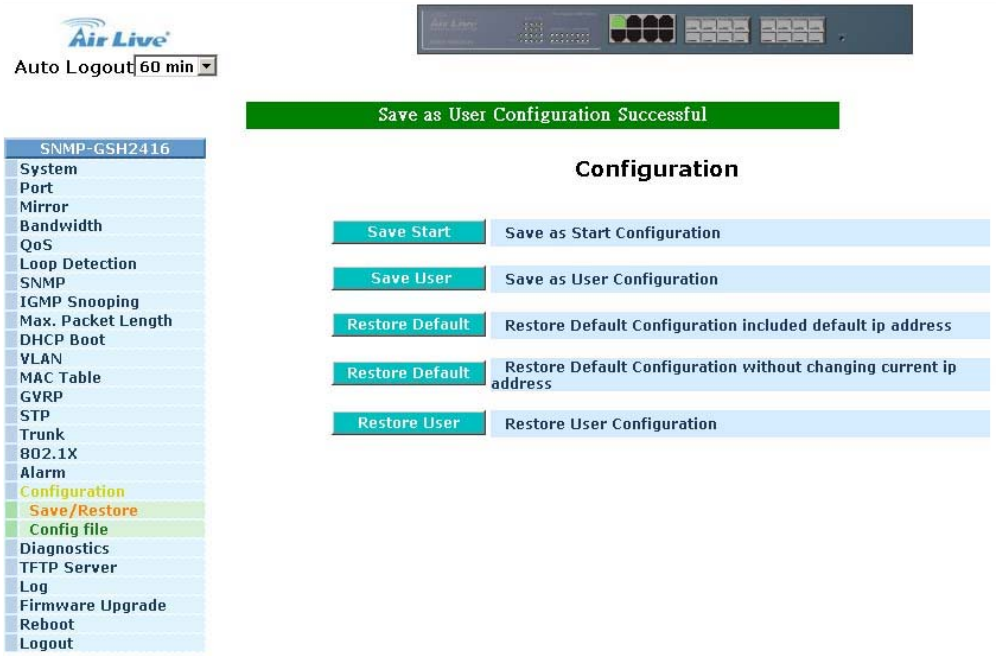

Auto Logout 60 min
Save as User Configuration Successful
SNMP-GSH2416
System
Port
Mirror
Bandwidth
QoS
Loop Detection
SNMP
IGMP Snooping
Max. Packet Length
DHCP Boot
VLAN
MAC Table
GVRP
STP
Trunk
802.1X
Alarm
Configuration
Save/Restore
Config file
Diagnostics
TFTP Server
Log
Firmware Upgrade
Reboot
Logout
Configuration
Save Start
Save as Start Configuration
Save User
Save as User Configuration
Restore Default
Restore Default Configuration included default ip address
Restore Default
Restore Default Configuration without changing current ip address
Restore User
Restore User Configuration

Fig. 3-64

Function name:

Restore Default Configuration (includes default IP address)

Function description:

Restore Default Configuration function can retrieve the ex-factory setting to replace the start configuration. And the IP address of the switch will also be restored to 192.168.1.1.

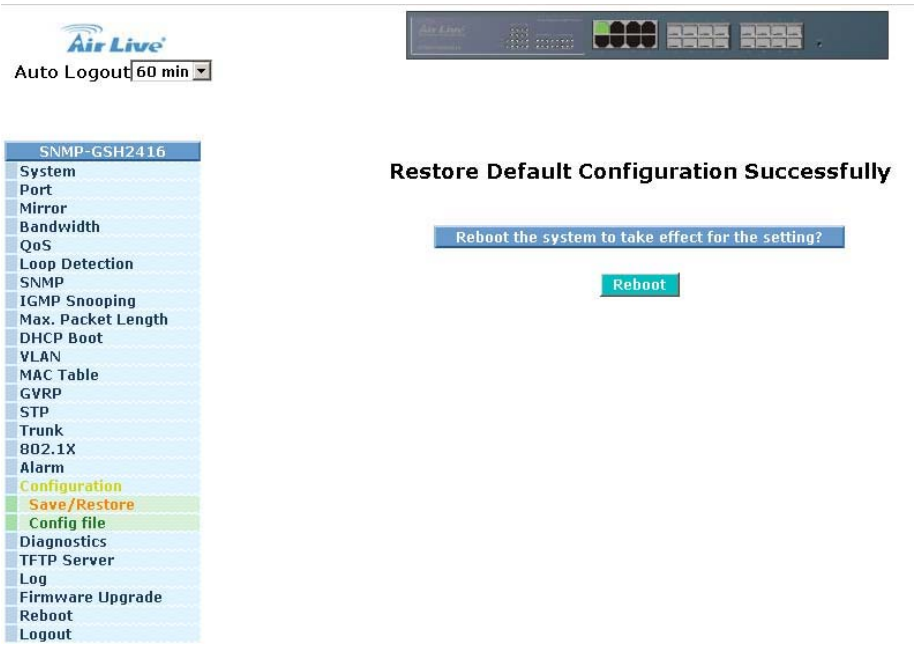


Fig. 3-65

Function name:

Restore Default Configuration (excludes current IP address)

Function description:

Restore Default Configuration function can retrieve the ex-factory setting to replace the start configuration. However, the switch's current IP address that the user set up will not be changed and will NOT be restored to 192.168.1.1 as well.

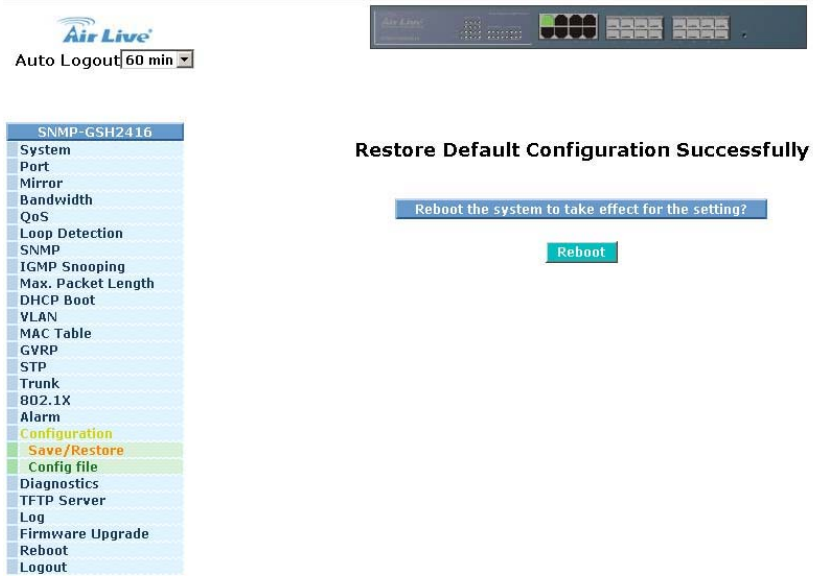

Air Live
Auto Logout 60 min
SNMP-GSH2416
System
Port
Mirror
Bandwidth
QoS
Loop Detection
SNMP
IGMP Snooping
Max. Packet Length
DHCP Boot
VLAN
MAC Table
GVRP
STP
Trunk
802.1X
Alarm
Configuration
Save/Restore
Config file
Diagnostics
TFTP Server
Log
Firmware Upgrade
Reboot
Logout
Restore Default Configuration Successfully
Reboot the system to take effect for the setting?
Reboot

Fig. 3-66

Function name:

Restore User Configuration

Function description:

Restore User Configuration function can retrieve the previous confirmed working configuration stored in the flash memory to update start configuration. When completing to restore the configuration, the system's start configuration is updated and will be changed its system settings after rebooting the system.

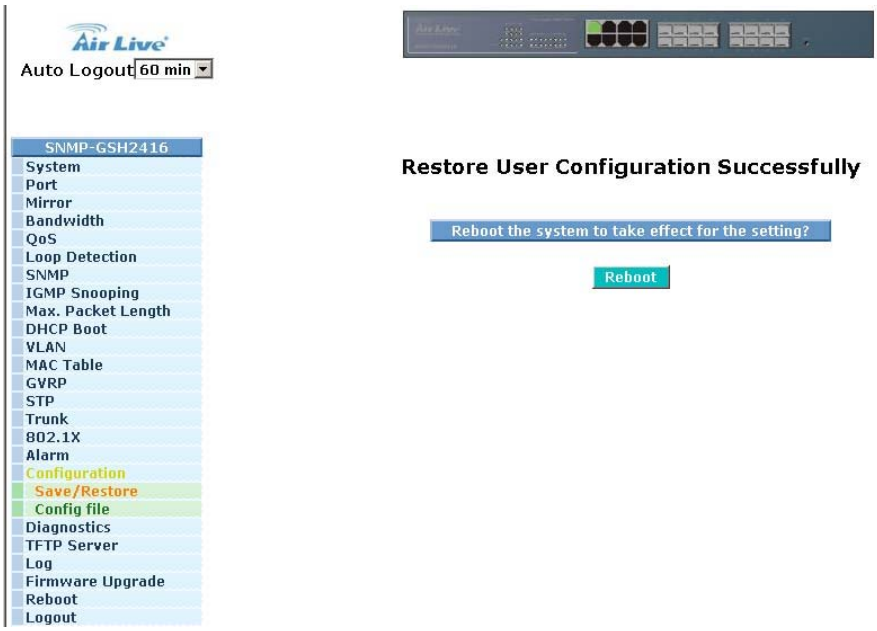


Fig. 3-67

3-17-2. Config File

Function name:

Config File

Function description:

With this function, user can back up or reload the config files of Save As Start or Save As User via TFTP.

Parameter description:

Export File Path:

Export Start:

Export Save As Start's config file stored in the flash.

Export User-Conf:

Export Save As User's config file stored in the flash.

Import File Path:

Import Start:

Import Save As Start's config file stored in the flash.

Import User-Conf:

Import Save As User's config file stored in the flash.

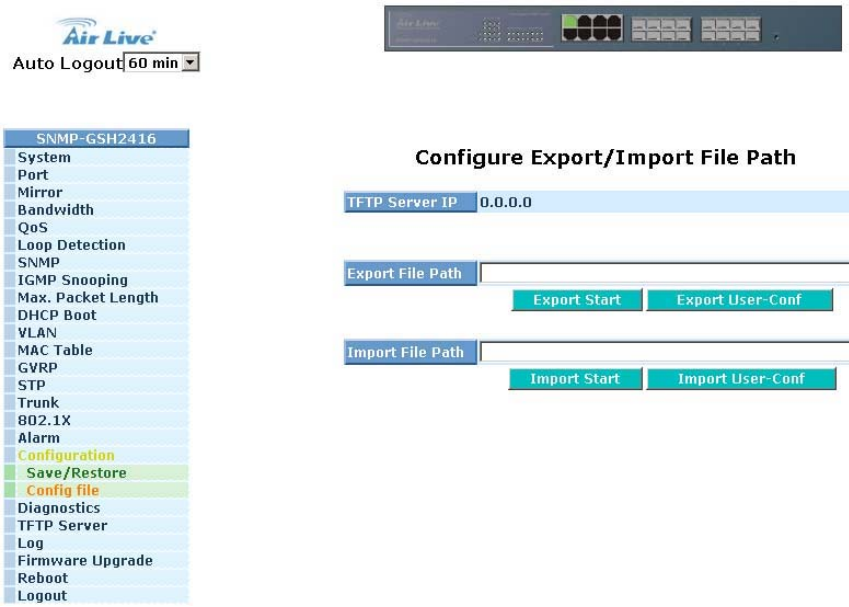
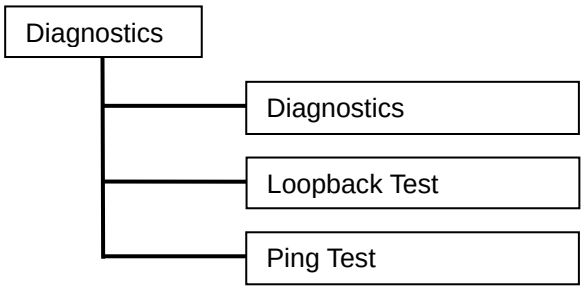


Fig. 3-68

3-18. Diagnostics

Three functions, including Diagnostics, Loopback Test and Ping Test are contained in this function folder for device self-diagnostics. Each of them will be described in detail orderly in the following sections.



Function name:

Diagnostics

Function description:

Diagnostics function provides a set of basic system diagnosis. It let users know that whether the system is health or needs to be fixed. The basic system check includes EEPROM test, UART test, DRAM test and Flash test.

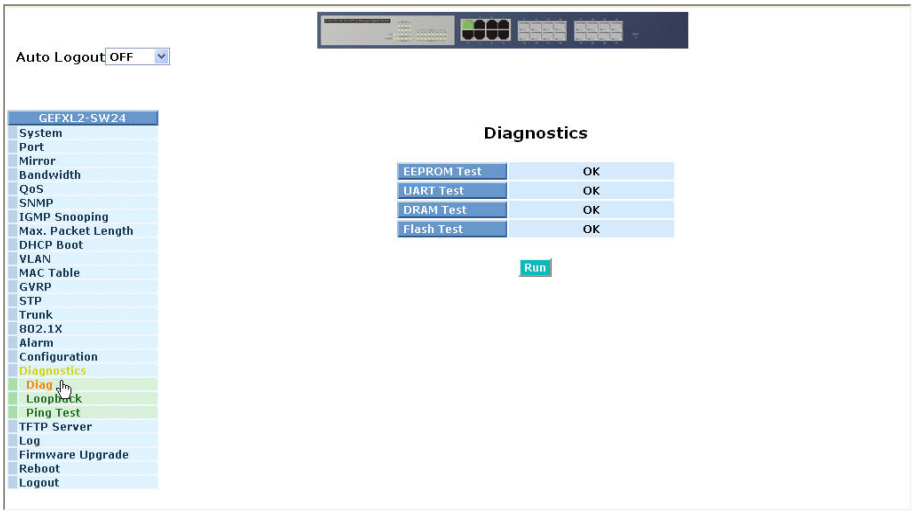


Fig. 3-69

Function name:

Loopback Test

Function description:

In the Loopback Test function, there are two different loopback tests. One is Internal Loopback Test and the other is External Loopback Test. The former test function will not send the test signal outside the switch box. The test signal only wraps around in the switch box. As to the latter test function, it will send the test signal to its link partner. If you do not have them connected to active network devices, i.e. the ports are link down, the switch will report the port numbers failed. If they all are ok, it just shows OK.

Note: Whatever you choose Internal Loopback Test or External Loopback Test, these two functions will interfere with the normal system working, and all packets in sending and receiving also will stop temporarily.

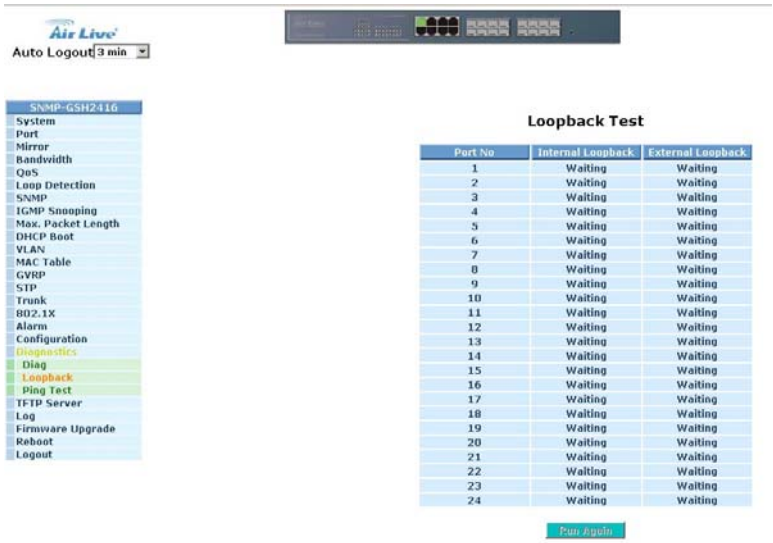


Fig. 3-70

Function name:

Ping Test

Function description:

Ping Test function is a tool for detecting if the target device is alive or not through ICMP protocol which abounds with report messages. The switch provides Ping Test function to let you know that if the target device is available or not. You can simply fill in a known IP address and then click **<Ping>** button. After a few seconds later, the switch will report you the pinged device is alive or dead in the field of Ping Result.

Parameter description:

IP Address:

An IP address with the version of v4, e.g. 192.168.1.1.

Default Gateway:

IP address of the default gateway.

For more details, please see the section of IP address in Chapter 2.

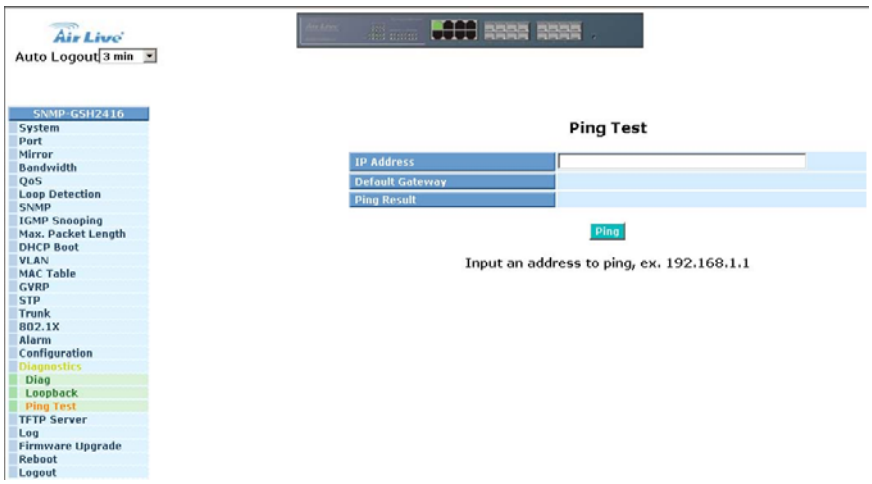


Fig. 3-71

3-19. TFTP Server

Function name:

TFTP Server

Function description:

Set up IP address of TFTP server.

Parameter description:

Specify the IP address where the TFTP server locates. Fill in the IP address of your TFTP server, then press **<Apply>** button to have the setting taken effect.

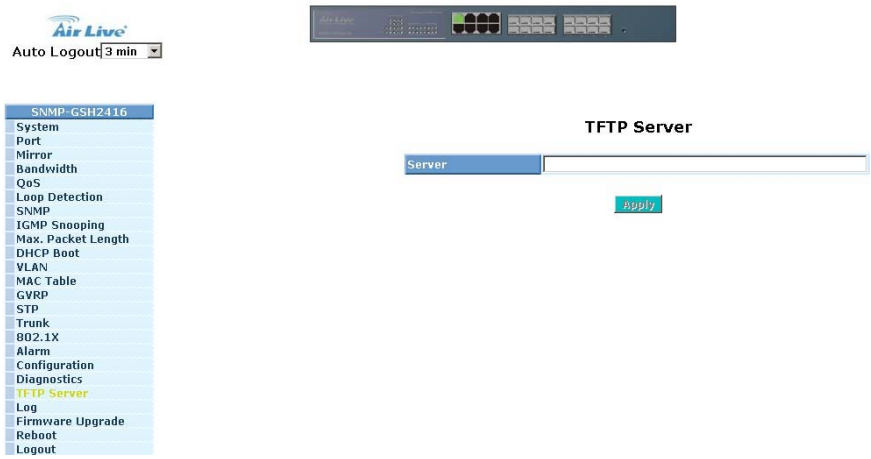


Fig. 3-72

3-20. Log

This function shows the log data. The switch provides system log data for users. There are 18 private trap logs, 5 public trap logs. The switch supports total 120 log entries. For more details on log items, please refer to the section of Trap/Alarm Configuration and SNMP Configuration.

Function name:

Log Data

Function description:

The Trap Log Data is displaying the log items including all SNMP Private Trap events, SNMP Public traps and user logs occurred in the system. In the report table, No., Time and Events are three fields contained in each trap record.

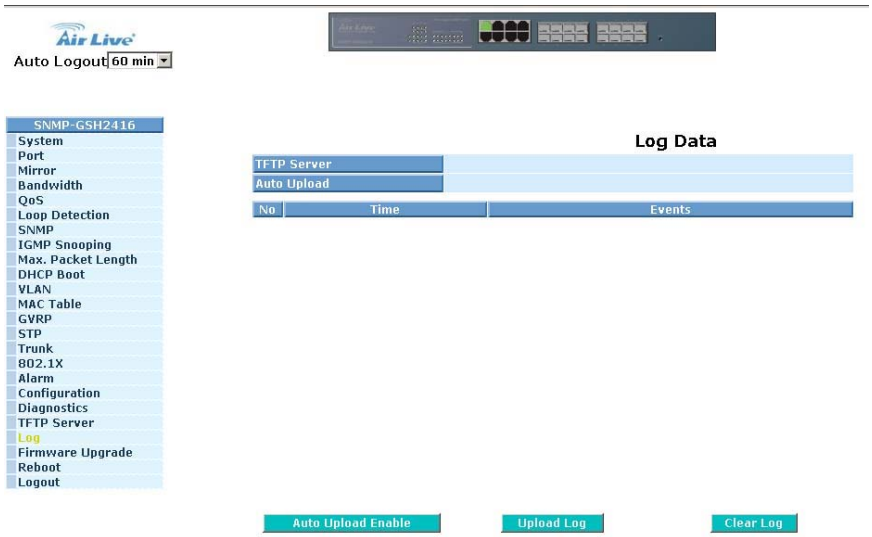


Fig. 3-73

Parameter description:

No.:

Display the order number that the trap happened.

Time:

Display the time that the trap happened.

Events:

Display the trap event name.

Auto Upload Enable:

Switch the enabled or disabled status of the auto upload function.

Upload Log:

Upload log data through tftp.

Clear Log:

Clear log data.

3-21. Firmware Upgrade

Software upgrade tool is used to help upgrade the software function in order to fix or improve the function. The switch provides a TFTP client for software upgrade. This can be done through Ethernet.

Function name:

Firmware Upgrade

Function description:

The switch supports TFTP upgrade tool for upgrading software. If you assure to upgrade software to a newer version one, you must follow two procedures:

1.) Specifying the IP address where TFTP server locates. In this field, the IP address of your TFTP server should be filled in.

2.) Specifying what the filename and where the file is. You must specify full path and filename.

Then, press **<Upgrade>** button if your download is not successful, the switch will also be back to “Software Upgrade”, and it will not upgrade the software as well.

When download is completed, the switch starts upgrading software. A reboot message will be prompted after completing upgrading software. At this time, you must reboot the switch to have new software worked.

Note: Software upgrade is hazardous if power is off. You must do it carefully.

Parameter description:

TFTP Server: A TFTP server stored the image file you want to upgrade.

Path and Filename: File path and filename stored the image file you want to upgrade.

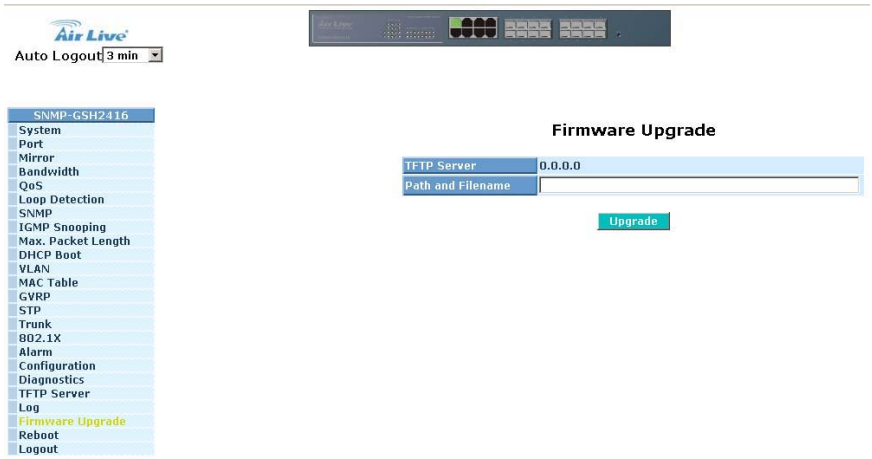


Fig. 3-74

3-22. Reboot

We offer you many ways to reboot the switch, including power up, hardware reset and software reset. You can press the RESET button in the front panel to reset the switch. After upgrading software, changing IP configuration or changing VLAN mode configuration, then you must reboot to have the new configuration taken effect. Here we are discussing is software reset for the “reboot” in the main menu.

Function name:

Reboot

Function description:

Reboot the switch. Reboot takes the same effect as the RESET button on the front panel of the switch. It will take around thirty (30) seconds to complete the system boot.

Parameter description:

Save and Reboot:

Save the current settings as start configuration before rebooting the switch.

Reboot:

Reboot the system directly.

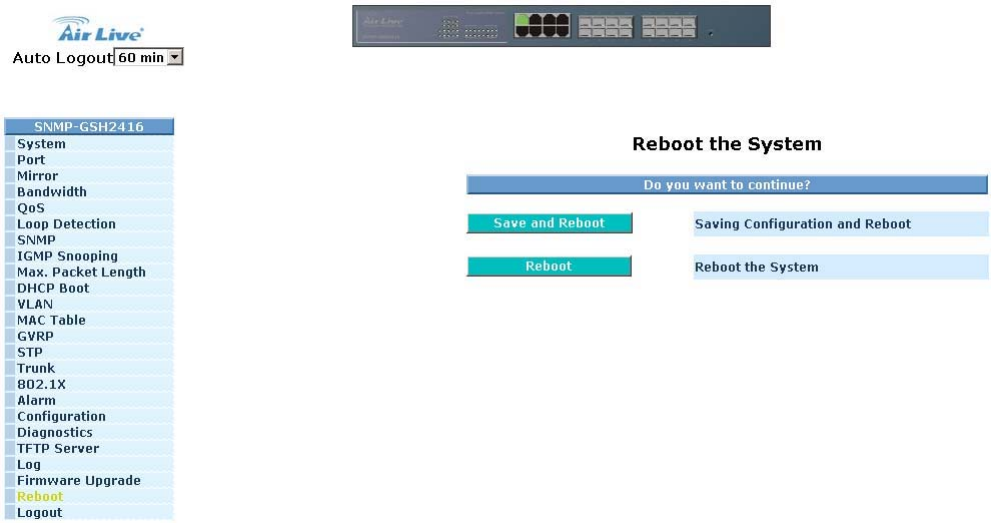


Fig. 3-75

3-23. Logout

You can manually logout by performing Logout function. In the switch, it provides another way to logout. You can configure it to logout automatically.

Function name:

Logout

Function description:

The switch allows you to logout the system to prevent other users from the system without the permission. If you do not logout and exit the browser, the switch will automatically have you logout. Besides this manually logout and implicit logout, you can pull down the **<Auto Logout>** list at the top-left corner to explicitly ON/OFF this logout function.

Parameter description:

Auto Logout:

Default is ON. If it is “ON”, and no action and no key is stroke as well in any function screen more than 3 minutes, the switch will have you logout automatically.

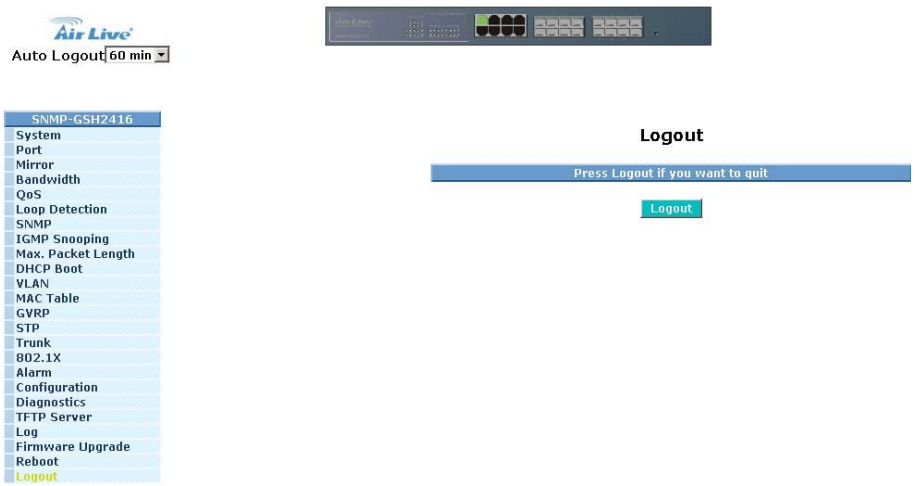


Fig. 3-76

4. Operation of CLI Management

4-1. CLI Management

Refer to Chapter 2 for basic installation. The following description is the brief of the network connection.

-- Locate the correct DB-9 null modem cable with female DB-9 connector. Null modem cable comes with the management switch. Refer to the Appendix B for null modem cable configuration.

-- Attach the DB-9 female connector to the male DB-9 serial port connector on the Management board.

-- Attach the other end of the DB-9 cable to an ASCII terminal emulator or PC Com-1, 2 port. For example, PC runs Microsoft Windows HyperTerminal utility.

-- At “Com Port Properties” Menu, configure the parameters as below: (see the next section)

Baud rate	57600
Stop bits	1
Data bits	8
Parity	N
Flow control	none

4-1-1. Login

The command-line interface (CLI) is a text-based interface. User can access the CLI through either a direct serial connection to the device or a Telnet session. The default values of the managed switch are listed below:

Username: admin
Password: admin

After you login successfully, the prompt will be shown as “**#**“ if you are the first login person and your authorization is administrator; otherwise it may show “**$**“. See the following two figures. The former means you behave as an administrator and have the access right of the system. As to the latter, it means you behave as a guest and are only allowed to view the system without the permission to do any setting for this switch.

```
L2 Managed Switch - SNMP-GSH2416

Login: admin
Password:
SNMP-GSH2416#
```

Fig. 4-1

```
L2 Managed Switch - SNMP-GSH2416

Login: admin
Password:

SNMP-GSH2416$
```

Fig. 4-2

4-2. Commands of CLI

To see the commands of the mode, please input "**?**" after the prompt, then all commands will be listed in the screen. All commands can be divided into two categories, including global commands and local commands. Global commands can be used wherever the mode you are. They are "exit", "end", "help", "history", "logout", "save start", "save user", "restore default" and "restore user". For more details, please refer to Section 4-2-1.

Command instructions reside in the corresponding modes are local commands. The same command with the same command name may occur but perform totally different function in different modes. For example, "show" in IP mode performs displaying the IP information; however, it performs displaying the system information in system mode. For more details, please refer to Section 4-2-2.

```
L2 Managed Switch -  SNMP-GSH2416

Login: admin
Password:

SNMP-GSH2416 # ?
  802.1X                Enter into 802.1X mode
  account               Enter into account mode
  alarm                 Enter into alarm mode
  autologout            Change autologout time
  bandwidth             Enter into bandwidth mode
  config-file           Enter into config file mode
  dhcp-boot             Enter into dhcp-boot mode
  diag                  Enter into diag mode
  firmware              Enter into firmware mode
  gvrp                  Enter into gvrp mode
  hostname              Change hostname
  igmp-snooping         Enter into igmp mode
  ip                    Enter into ip mode
  log                   Enter into log mode
  mac-table             Enter into mac table mode
  management            Enter into management mode
  max-pkt-len           Enter into max packet length mode
  mirror                Enter into mirror mode
```

Fig. 4-3

4-2-1. Global Commands of CLI

end

Syntax:
end
Description:
Back to the top mode.
When you enter this command, your current position would move to the top mode. If you use this command in the top mode, you are still in the position of the top mode.
Argument:
None.
Possible value:
None.
Example:

```
SNMP-GSH2416# alarm
SNMP-GSH2416(alarm)# events
SNMP-GSH2416(alarm-events)# end

SNMP-GSH2416#
```

exit

Syntax:
exit
Description:
Back to the previous mode.
When you enter this command, your current position would move back to the previous mode. If you use this command in the top mode, you are still in the position of the top mode.
Argument:
None.
Possible value:
None.
Example:

```
SNMP-GSH2416# trunk
SNMP-GSH2416(trunk)# exit

SNMP-GSH2416#
```

help

Syntax:
help
Description:
To show available commands.
Some commands are the combination of more than two words. When you enter this command, the CLI would show the complete commands. Besides, the command would help you classify the commands between the local commands and the global ones.
Argument:
None.
Possible value:
None.
Example:

```
SNMP-GSH2416# ip
SNMP-GSH2416(ip)# help
Commands available:
  ------------<< Local commands >>------------
  set ip               Set ip,subnet mask and gateway
  set dns              Set dns
  enable dhcp          Enable DHCP, and set dns auto or manual
  disable dhcp         Disable DHCP
  show                 Show IP Configuration
  ------------<< Global commands >>------------
  exit                 Back to the previous mode
  end                  Back to the top mode
  help                 Show available commands
  history              Show a list of previously run commands
  logout               Logout the system
  save start           Save as start config
  save user            Save as user config
  restore default      Restore default config
  restore user         Restore user config
```

history

Syntax:
history [#]
Description:
To show a list of previous commands that you had ever run.
When you enter this command, the CLI would show a list of commands which you had typed before. The CLI supports up to 256 records. If no argument is typed, the CLI would list total records up to 256. If optional argument is given, the CLI would only show the last numbers of records, given by the argument.
Argument:
[#]: show last number of history records. (optional)
Possible value:
[#]: 1, 2, 3, …., 256
Example:

```
SNMP-GSH2416(ip)# history
 Command history:
  0. trunk
  1. exit
  2. SNMP-GSH2416# trunk
  3. SNMP-GSH2416(trunk)# exit
  4. SNMP-GSH2416#
  5. ?
  6. trunk
  7. exit
  8. alarm
  9. events
 10. end
 11. ip
 12. help
 13. ip
 14. history

SNMP-GSH2416(ip)# history 3
 Command history:
 13. ip
 14. history
 15. history 3

SNMP-GSH2416(ip)#
```

logout

Syntax:
logout
Description:
When you enter this command via Telnet connection, you would logout the system and disconnect. If you connect the system through direct serial port with RS-232 cable, you would logout the system and be back to the initial login prompt when you run this command.
Argument:
None.
Possible value:
None.
Example:
SNMP-GSH2416# logout

restore default

Syntax:
restore default
Description:
When you use this function in CLI, the system will show you the information “Do you want to restore the default IP address?(y/n)”. If you choose Y or y, the IP address will restore to default “192.168.1.1”. If you choose N or n, the IP address will keep the same one that you had saved before.

If restoring default successfully, the CLI would prompt if reboot immediately or not. If you press Y or y, the system would reboot immediately; otherwise, it would be back to the CLI system. After restoring default configuration, all the changes in the startup configuration would be lost. After rebooting, the entire startup configuration would reset to factory default.

Argument:
None.
Possible value:
None.
Example:
SNMP-GSH2416# restore default
Restoring ...
Restore Default Configuration Successfully
Press any key to reboot system.

restore user

Syntax:
restore user
Description:
To restore the startup configuration as user defined configuration. If restoring default successfully, the CLI would prompt if reboot immediately or not. If you press Y or y, the system would reboot immediately; others would back to the CLI system. After restoring user-defined configuration, all the changes in the startup configuration would be lost. After rebooting, the entire startup configuration would replace as user defined one.
Argument:
None.
Possible value:
None.
Example:
SNMP-GSH2416# restore user
Restoring ...
Restore User Configuration Successfully
Press any key to reboot system.

save start

Syntax:
save start
Description:
To save the current configuration as the start one. When you enter this command, the CLI would save your current configuration into the non-volatile FLASH. If you want the configuration still works after rebooting, save the configuration using the command ‘save stat’.
Argument:
None.
Possible value:
None.
Example:
SNMP-GSH2416# save start
Saving start...
Save Successfully

SNMP-GSH2416#

save user

Syntax:
save user
Description:
To save the current configuration as the user-defined configuration. When you enter this command, the CLI would save your current configuration into the non-volatile FLASH as user-defined configuration.
Argument:
None.
Possible value:
None.
Example:
SNMP-GSH2416# save user
Saving user...
Save Successfully

SNMP-GSH2416#

4-2-2. Local Commands of CLI

■ 802.1X

set max-request

Syntax:
set max-request <port-range> <times>
Description:
The maximum number of times that the state machine will retransmit an EAP Request packet to the Supplicant before it times out the authentication session.
Argument:
<port range> : syntax 1,5-7, available from 1 to 24
<times>: max-times , range 1-10
Possible value:
<port range> : 1 to 24
<times>: 1-10, default is 2
Example:
SNMP-GSH2416(802.1X)# set max-request 2 2

set mode

Syntax:
set mode <port-range> <mode>
Description:
To set up the 802.1X authentication mode of each port.
Argument:
<port range> : syntax 1,5-7, available from 1 to 24
<mode>: set up 802.1X mode
0:disable the 802.1X function
1:set 802.1X to Multi-host mode
Possible value:
<port range> : 1 to 24
<mode>: 0 or 1
Example:
SNMP-GSH2416(802.1X)# set mode 2 1

set port-control

Syntax:
set port-control <port-range> <authorized>
Description:
To set up 802.1X status of each port.
Argument:
<port range> : syntax 1,5-7, available from 1 to 24
<authorized> : Set up the status of each port
0:ForceUnauthorized
1:ForceAuthorized
2:Auto
Possible value:
<port range> : 1 to 24
<authorized> : 0, 1 or 2
Example:
SNMP-GSH2416(802.1X)# set port-control 2 2

set quiet-period

Syntax:
set quiet-period <port-range> <sec>
Description:
A timer used by the Authenticator state machine to define periods of time during when it will not attempt to acquire a Supplicant.
Argument:
<port range> : syntax 1,5-7, available from 1 to 24
<sec> : timer , range 0-65535
Possible value:
<port range> : 1 to 24
<sec> : 0-65535, default is 60
Example:
SNMP-GSH2416(802.1X)# set quiet-period 2 30

set reAuthEnabled

Syntax:
set reAuthEnabled <port-range> <ebl>
Description:
A constant that define whether regular reauthentication will take place on this port.
Argument:
<port range> : syntax 1,5-7, available from 1 to 24
<ebl> :
0:OFF Disable reauthentication
1:ON Enable reauthentication
Possible value:
<port range> : 1 to 24
<ebl> : 0 or 1, default is 1
Example:
SNMP-GSH2416(802.1X)# set reAuthEnabled 2 1

set reAuthMax

Syntax:
set reAuthMax <port-range> <max>
Description:
The number of reauthentication attempts that are permitted before the port becomes Unauthorized.
Argument:
<port range> : syntax 1,5-7, available from 1 to 24
<max> : max. value , range 1-10
Possible value:
<port range> : 1 to 24
<max> : 1-10, default is 2
Example:
SNMP-GSH2416(802.1X)# set reAuthMax 2 2

set reAuthPeriod

Syntax:
set reAuthPeriod <port-range> <sec>
Description:
A constant that defines a nonzero number of seconds between periodic reauthentication of the supplicant.
Argument:
<port range> : syntax 1,5-7, available from 1 to 24
<sec> : timer , range 1-65535
Possible value:
<port range> : 1 to 24
<sec> : 1-65535, default is 3600
Example:
SNMP-GSH2416(802.1X)# set reAuthPeriod 2 3600

set serverTimeout

Syntax:
set serverTimeout <port-range> <sec>
Description:
A timer used by the Backend Authentication state machine in order to determine timeout conditions in the exchanges between the Authenticator and the Supplicant or Authentication Server. The initial value of this timer is either suppTimeout or serverTimeout, as determined by the operation of the Backend Authentication state machine.
Argument:
<port range> : syntax 1,5-7, available from 1 to 24
<sec> : timer , range 1-65535
Possible value:
<port range> : 1 to 24
<sec> : 1-65535, default is 30
Example:
SNMP-GSH2416(802.1X)# set serverTimeout 2 30

set state

Syntax:

set state <ip> <port-number> <secret-key>
Description:
To configure the settings related with 802.1X Radius Server.
Argument:
<ip> : the IP address of Radius Server
<port-number> : the service port of Radius Server(Authorization port)
<secret-key> : set up the value of secret-key, and the length of secret-key is from 1 to 31
Possible value:
<port-number> : 1~65535, default is 1812
Example:
SNMP-GSH2416(802.1X)# set state 192.168.1.115 1812 WinRadius

set suppTimeout

Syntax:
set suppTimeout <port-range> <sec>
Description:
A timer used by the Backend Authentication state machine in order to determine timeout conditions in the exchanges between the Authenticator and the Supplicant or Authentication Server. The initial value of this timer is either suppTimeout or serverTimeout, as determined by the operation of the Backend Authentication state machine.
Argument:
<port range> : syntax 1,5-7, available from 1 to 24
<sec> : timer , range 1-65535
Possible value:
<port range> : 1 to 24
<sec> : 1-65535, default is 30
Example:
SNMP-GSH2416(802.1X)# set suppTimeout 2 30

set txPeriod

Syntax:
set txPeriod <port-range> <sec>
Description:
A timer used by the Authenticator PAE state machine to determine when an EAPOL PDU is to be transmitted
Argument:
<port range> : syntax 1,5-7, available from 1 to 24
<sec> : timer , range 1-65535
Possible value:
<port range> : 1 to 24
<sec> : 1-65535, default is 30
Example:
SNMP-GSH2416(802.1X)# set txPeriod 2 30

show mode

Syntax:
show mode
Description:

To display the mode of each port.
Argument:
None.
Possible value:
None.
Example:
SNMP-GSH2416(802.1X)# show mode
```
 Port     Mode
====== ============
  1     Disable
  2     Multi-host
  3     Disable
  4     Disable
  5     Disable
  6     Disable
        :
        :
        :
```

show parameter

Syntax:
show parameter
Description:
To display the parameter settings of each port.
Argument:
None.
Possible value:
None.
Example:
SNMP-GSH2416(802.1X)# show parameter
```
port  1) port control  : Auto
         reAuthMax     : 2
         txPeriod      : 30
         Quiet Period  : 60
         reAuthEnabled : ON
         reAuthPeriod  : 3600
         max. Request  : 2
         suppTimeout   : 30
         serverTimeout : 30
```

```
port  2) port control  : Auto
          reAuthMax     : 2
          txPeriod      : 30
          Quiet Period  : 60
          reAuthEnabled : ON
          reAuthPeriod  : 3600
          max. Request  : 2
          suppTimeout   : 30
          serverTimeout : 30
                :
                :
                :
```

show security

Syntax:
show security
Description:
To display the authentication status of each port.
Argument:
None.
Possible value:
None.
Example:
SNMP-GSH2416(802.1X)# show security

```
 Port      Mode          Status
====== ============ ==============
   1     Disable
   2     Multi-host   Unauthorized
   3     Disable
   4     Disable
   5     Disable
   6     Disable
            :
            :
```

show state

Syntax:
show state
Description:
Show the Radius server configuration
Argument:
None.
Possible value:
None.
Example:
SNMP-GSH2416(802.1X)# show state

```
Radius Server: 192.168.1.115
Port Number  : 1812
Secret Key   : WinRadius
```

■ account

add

Syntax:
add <name>
Description:
To create a new guest user. When you create a new guest user, you must type in password and confirm password.
Argument:
<name> : new account name
Possible value:
A string must be at least 5 character.
Example:

```
SNMP-GSH2416(account)# add aaaaa
Password:
Confirm Password:
Save Successfully
SNMP-GSH2416(account)#
```

del

Syntax:
del <name>
Description:
To delete an existing account.
Argument:
<name> : existing user account
Possible value:
None.
Example:

```
SNMP-GSH2416(account)# del aaaaa
Account aaaaa deleted
```

modify

Syntax:
modify <name>
Description:
To change the username and password of an existing account.
Argument:
<name> : existing user account
Possible value:
None.
Example:

```
SNMP-GSH2416(account)# modify aaaaa
username/password: the length is from 5 to 15.
Current username (aaaaa):bbbbb
New password:
Confirm password:
Username changed successfully.
Password changed successfully.
```

show

Syntax:
show
Description:
To show system account, including account name and identity.
Argument:
None.
Possible value:
None.
Example:

```
SNMP-GSH2416(account)# show
Account Name       Identity
---------------- ---------------
 admin              Administrator
 guest                  guest
```

■ alarm

<<email>>

del mail-address

Syntax:
del mail-address <#>
Description:
To remove the configuration of E-mail address.
Argument:
<#>: email address number, range: 1 to 6
Possible value:
<#>: 1 to 6
Example:
```
SNMP-GSH2416(alarm-email)# del mail-address 2
```

del server-user

Syntax:
del server-user
Description:
To remove the configuration of server, user account and password.
Argument:
None.
Possible value:
None.
Example:
```
SNMP-GSH2416(alarm-email)# del server-user
```

set mail-address

Syntax:
set mail-address <#> <mail address>
Description:
To set up the email address.
Argument:
<#> :email address number, range: 1 to 6
<mail address>:email address
Possible value:
<#>: 1 to 6
Example:
```
SNMP-GSH2416(alarm-email)# set mail-address 1  abc@mail.abc.com
```

set server

Syntax:
set server <ip>
Description:
To set up the IP address of the email server.
Argument:
<ip>:email server ip address or domain name
Possible value:
None.
Example:
```
SNMP-GSH2416(alarm-email)# set server 192.168.1.6
```

set user

Syntax:
set user <username>
Description:
To set up the account and password of the email server.
Argument:
<username>: email server account and password
Possible value:
None.
Example:
```
SNMP-GSH2416 (alarm-email)# set user admin
```

show

Syntax:
show
Description:
To display the configuration of e-mail.
Argument:
None.
Possible value:
None.
Example:
```
SNMP-GSH2416(alarm-email)# show
Mail Server    : 192.168.1.6
Username       : admin
Password       : ****************
Email Address 1: abc@mail.abc.com
Email Address 2:
Email Address 3:
Email Address 4:
Email Address 5:
Email Address 6:
```

<<events>>

del all

Syntax:
del all <range>
Description:
To disable email, sms and trap of events.
Argument:
<range>:del the range of events, syntax 1,5-7
Possible value:
<range>: 1~23
Example:
SNMP-GSH2416(alarm-events)# del all 1-3

del email

Syntax:
del email <range>
Description:
To disable the email of the events.
Argument:
<range>:del the range of email, syntax 1,5-7
Possible value:
<range>: 1~23
Example:
SNMP-GSH2416(alarm-events)# del email 1-3

del sms

Syntax:
del sms <range>
Description:
To disable the sms of the events.
Argument:
<range>:del the range of sms, syntax 1,5-7
Possible value:
<range>: 1~23
Example:
SNMP-GSH2416(alarm-events)# del sms 1-3

del trap

Syntax:
del trap <range>
Description:
To disable the trap of the events.
Argument:
<range>:del the range of trap, syntax 1,5-7
Possible value:
<range>: 1~23
Example:
```
SNMP-GSH2416(alarm-events)# del trap 1-3
```

set all

Syntax:
set all <range>
Description:
To enable email, sms and trap of events.
Argument:
<range>:set the range of events, syntax 1,5-7
Possible value:
<range>: 1~23
Example:
```
SNMP-GSH2416(alarm-events)# set all 1-3
```

set email

Syntax:
set email <range>
Description:
To enable the email of the events.
Argument:
<range>:set the range of email, syntax 1,5-7
Possible value:
<range>: 1~23
Example:
```
SNMP-GSH2416(alarm-events)# set email 1-3
```

set sms

Syntax:
set sms <range>
Description:
To enable the sms of the events.
Argument:
<range>:set the range of sms, syntax 1,5-7
Possible value:
<range>: 1~23
Example:
SNMP-GSH2416(alarm-events)# set sms 1-3

set trap

Syntax:
set trap <range>
Description:
To enable the trap of the events.
Argument:
<range>:set the range of trap, syntax 1,5-7
Possible value:
<range>: 1~23
Example:
SNMP-GSH2416(alarm-events)# set trap 1-3

show

Syntax:
show
Description:
To display the configuration of alarm event.
Argument:
None.
Possible value:
None.

Example:

```
SNMP-GSH2416(alarm-events)# show
   Events                    Email SMS Trap
-----------------------------------------
1  Cold Start                          v
2  Warm Start                          v
3  Link Down                           v
4  Link Up                             v
5  Authentication Failure              v
6  User Login
7  User Logout
8  STP Topology Changed
9  STP Disabled
10 STP Enabled
11 LACP Disabled
12 LACP Enabled
13 LACP Member Added
14 LACP Port Failure
15 GVRP Disabled
16 GVRP Enabled
17 VLAN Disabled
18 Port-based Vlan Enabled
19 Tag-based Vlan Enabled
20 Metro-mode Vlan Enabled
21 Double-tag Vlan Enabled
22 Module Inserted
23 Module Removed
```

show (alarm)

Syntax:
show
Description:
The Show for alarm here is used to display the configuration of Trap, SMS or E-mail.
Argument:
None.
Possible value:
None.
Example:
```
SNMP-GSH2416(alarm)# show events
SNMP-GSH2416(alarm)# show email
SNMP-GSH2416(alarm)# show sms
```

<<sms>>

del phone-number

Syntax:
del phone-number <#>
Description:
To delete sms phone number.
Argument:
<#>: mobile phone number, range: 1 to 6
Possible value:
<#>: 1 to 6
Example:
```
SNMP-GSH2416(alarm-sms)# del phone-number 3
```

del server-user

Syntax:
del server-user
Description:
To delete sms server, user account and password.
Argument:
None.
Possible value:
None.
Example:
```
SNMP-GSH2416(alarm-sms)# del server-user
```

set phone-number

Syntax:
set phone-number <#> <phone-number>
Description:
To add sms phone number.
Argument:
<#>: mobile phone number, range: 1 to 6
<phone-number>: phone number
Possible value:
<#>: 1 to 6
Example:
SNMP-GSH2416(alarm-sms)# set phone-number 1 0968777777

set server

Syntax:
set server <ip>
Description:
To set up the IP address of sms server.
Argument:
<ip>: SMS server ip address or domain name
Possible value:
None.
Example:
SNMP-GSH2416(alarm-sms)# set server 192.168.1.7

set user

Syntax:
set user <username>
Description:
To set up user account and password of sms server.
Argument:
<username>: SMS server account
Possible value:
None.
Example:
SNMP-GSH2416(alarm-sms)# set user ABC

show

Syntax:
show
Description:
To display the configuration of SMS trap event.
Argument:
None.
Possible value:
None.
Example:

```
SNMP-GSH2416(alarm-sms)# show
SMS Server      : 192.168.1.7
Username        : ABC
Password        : ****************
Mobile Phone  1: 0968777777
Mobile Phone  2:
Mobile Phone  3:
Mobile Phone  4:
Mobile Phone  5:
Mobile Phone  6:
```

■ autologout

autologout

Syntax:
autologout <time>
Description:
To set up the timer of autologout.
Argument:
<time>: range 1 to 3600 seconds, 0 for autologout off, current setting is 180 seconds.
Possible value:
<time>: 0,1-3600
Example:
SNMP-GSH2416# autologout 3600
Set autologout time to 3600 seconds

■ bandwidth

disable egress-rate

Syntax:
disable egress-rate <range>
Description:
To cancel the egress-rate of the port.
Argument:
<range>:syntax 1,5-7, available from 1 to 24
Possible value:
<range>: 1 to 24
Example:
SNMP-GSH2416(bandwidth)# disable egress-rate 1-8

disable ingress-rate

Syntax:
disable ingress-rate <range>
Description:
To cancel the Ingress-rate of the port.
Argument:
<range>:syntax 1,5-7, available from 1 to 24
Possible value:
<range>: 1 to 24
Example:
SNMP-GSH2416(bandwidth)# disable ingress-rate 1-8

disable storm-rate

Syntax:
disable storm-rate <range>
Description:
To cancel the storm-rate of the port.
Argument:
<range>:syntax 1,5-7, available from 1 to 24
Possible value:
<range>: 1 to 24
Example:
SNMP-GSH2416(bandwidth)# disable storm-rate 1-8

enable egress-rate

Syntax:
enable egress-rate <range> <data_rate>
Description:
To set up the egress-rate of the port.
Argument:
<range>:syntax 1,5-7, available from 1 to 24
<data_rate>: 0-1000
Possible value:
<range>: 1 to 24
<data_rate>: 0-1000
Example:
SNMP-GSH2416(bandwidth)# enable egress-rate 1-16 200

enable ingress-rate

Syntax:
enable ingress-rate <range> <data_rate>
Description:
To set up the Ingress-rate of the ports.
Argument:
<range>:syntax 1,5-7, available from 1 to 24
<data_rate>: 0-1000
Possible value:
<range>: 1 to 24
<data_rate>: 0-1000
Example:
SNMP-GSH2416(bandwidth)# enable ingress-rate 1-16 100

enable storm-rate

Syntax:
enable storm-rate <range> <data_rate>
Description:
To set up the storm-rate of the ports.
Argument:
<range>:syntax 1,5-7, available from 1 to 24
<data_rate>: 0-1000
Possible value:
<range>: 1 to 24
<data_rate>: 0-1000
Example:
SNMP-GSH2416(bandwidth)# enable strom-rate 1-16 150

show

Syntax:
show
Description:
To display all current settings of the bandwidth.
Argument:
None.
Possible value:
None.
Example:
SNMP-GSH2416(bandwidth)# show

Port	Ingress				Egress	
	All State	All Rate	Storm State	Storm Rate	All state	All Rate
1	Disabled	0	Disabled	0	Disabled	0
2	Disabled	0	Disabled	0	Disabled	0
3	Disabled	0	Disabled	0	Disabled	0
4	Disabled	0	Disabled	0	Disabled	0
5	Disabled	0	Disabled	0	Disabled	0
6	Disabled	0	Disabled	0	Disabled	0
7	Disabled	0	Disabled	0	Disabled	0
8	Disabled	0	Disabled	0	Disabled	0
9	Disabled	0	Disabled	0	Disabled	0
10	Disabled	0	Disabled	0	Disabled	0
11	Disabled	0	Disabled	0	Disabled	0
12	Disabled	0	Disabled	0	Disabled	0
13	Disabled	0	Disabled	0	Disabled	0
14	Disabled	0	Disabled	0	Disabled	0
15	Disabled	0	Disabled	0	Disabled	0
16	Disabled	0	Disabled	0	Disabled	0
17	Disabled	0	Disabled	0	Disabled	0
18	Disabled	0	Disabled	0	Disabled	0
19	Disabled	0	Disabled	0	Disabled	0
20	Disabled	0	Disabled	0	Disabled	0

...(q to quit)

21	Disabled	0	Disabled	0	Disabled	0
22	Disabled	0	Disabled	0	Disabled	0
23	Disabled	0	Disabled	0	Disabled	0
24	Disabled	0	Disabled	0	Disabled	0

■ config-file

export start

Syntax:
export start
Description:
To run the export start function.
Argument:
None.
Possible value:
None.
Example:
SNMP-GSH2416(config-file)# export start
Export successful.

export user-conf

Syntax:
export user-conf
Description:
To run the export user-conf function.
Argument:
None
Possible value:
None
Example:
SNMP-GSH2416(config-file)# export user-conf
Export successful.

import start

Syntax:
import start
Description:
To run the import start function.
Argument:
None.
Possible value:
None.
Example:
SNMP-GSH2416(config-file)# import start
Import successful.

import user-conf

Syntax:
import user-conf
Description:
To run the import user-conf function.
Argument:
None.
Possible value:
None.
Example:
SNMP-GSH2416(config-file)# import user-conf
Import successful.

set export-path

Syntax:
set export-path <filepath>
Description:
To set up the filepath and filename that will be exported.
Argument:
<filepath>:filepath and filename
Possible value:
<filepath>:filepath and filename
Example:
SNMP-GSH2416(config-file)# set export-path log/21511.txt

set import-path

Syntax:
set import-path <filepath>
Description:
To set up the filepath and filename that will be imported.
Argument:
<filepath>:filepath and filename
Possible value:
<filepath>:filepath and filename
Example:
SNMP-GSH2416(config-file)# set import-path log/21511.txt

show

Syntax:
show
Description:
To display the config-file information.
Argument:
None.
Possible value:
None.
Example:
SNMP-GSH2416(config-file)# show
TFTP Server IP Address: 192.168.3.111
Export Path and Filename: nmap/123.ts
Import Path and Filename: user123.txt

■ dhcp-boot

set dhcp-boot

Syntax:
set dhcp-boot <sec>
Description:
To set up the delay time for DHCP Boot.
Argument:
<sec>:range syntax: 0, 1-30. The value “0” is to disable dhcp-boot delay
Possible value:
<sec>:0-30
Example:
SNMP-GSH2416(dhcp-boot)# set dhcp-boot 30

show

Syntax:
show
Description:
To display the status of DHCP Boot.
Argument:
None.
Possible value:
None.
Example:
SNMP-GSH2416(dhcp-boot)#show
dhcp boot : Enable
Second : 10

■ diag

diag

Syntax:
diag
Description:
Diag is used to test whether UART, DRAM, Flash and EEPROM is normal or not.
Argument:
None.
Possible value:
None.
Example:

```
SNMP-GSH2416(diag)# diag
EEPROM Test : OK
UART Test   : OK
DRAM Test   : OK
Flash Test  : OK
```

loopback

Syntax:
Loopback
Description:
For Internal/External Loopback Test.
Argument:
None.
Possible value:
None.
Example:

```
SNMP-GSH2416(diag)# loopback
Internal Loopback Test : OK

External Loopback Test : Port 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18
19 20 21 22 23 24 Fail
```

ping

Syntax:
ping <ip>
Description:
To confirm that whether the remote end-station or switch itself is alive or not.
Argument:
<ip> : ip address or domain name
Possible value:
IP address, e.g. 192.168.2.65 or domain name, e.g. tw.yahoo.com
Example:

```
SNMP-GSH2416(diag)# ping 192.168.1.115
Gateway      : 192.168.1.253
192.168.1.115 is alive.
```

■ firmware

set upgrade-path

Syntax:
set upgrade-path <filepath>
Description:
To set up the image file that will be upgraded.
Argument:
<filepath>: upgrade file path
Possible value:
<filepath>: upgrade file path
Example:
SNMP-GSH2416(firmware)# set upgrade-path gs2124c_SNMP-GSH2416_v2.03.img

show

Syntax:
show
Description:
To display the information of tftp server and upgrade-path.
Argument:
None.
Possible value:
None.
Example:
SNMP-GSH2416(firmware)# show
TFTP Server IP Address: 192.168.3.111
Path and Filename : gs2124c_SNMP-GSH2416_v2.03.img

upgrade

Syntax:
upgrade
Description:
To run the upgrade function.
Argument:
None.
Possible value:
None.
Example:
SNMP-GSH2416(firmware)# upgrade
Upgrading firmware ...

■ gvrp

disable

Syntax:
disable
Description:
To disable the gvrp function.
Argument:
None.
Possible value:
None.
Example:
SNMP-GSH2416(gvrp)# disable

enable

Syntax:
enable
Description:
To enable the gvrp function.
Argument:
None.
Possible value:
None.
Example:
SNMP-GSH2416(gvrp)# enable

group

Syntax:
group <group number>
Description:
To enter any of gvrp group for changing gvrp group setting. You can change the applicant or registrar mode of existing gvrp group per port.
Argument:
<group number>: enter which gvrp group you had created, using value is vid. Available range: 1 to 4094
Possible value:
<group number>: 1~4094
Example:

```
SNMP-GSH2416(gvrp)# show group
GVRP group information
Current Dynamic Group Number: 1
VID  Member Port
---- ------------------------------------------------
2    5
```

```
SNMP-GSH2416(gvrp)# group 2
SNMP-GSH2416(gvrp-group-2)# set applicant 1-6 non-participant

SNMP-GSH2416(gvrp-group-2)# show
GVRP group VID: 2
Port Applicant       Registrar
---- --------------- ---------
1    Non-Participant Normal
2    Non-Participant Normal
3    Non-Participant Normal
4    Non-Participant Normal
5    Non-Participant Normal
6    Non-Participant Normal
7    Normal          Normal
8    Normal          Normal
12   Normal          Normal
13   Normal          Normal
              :
              :
23   Normal          Normal
24   Normal          Normal


SNMP-GSH2416(gvrp-group-2)# set registrar 1-10 fixed

SNMP-GSH2416(gvrp-group-2)# show
GVRP group VID: 2
Port Applicant       Registrar
---- --------------- ---------
1    Non-Participant Fixed
2    Non-Participant Fixed
3    Non-Participant Fixed
4    Non-Participant Fixed
5    Non-Participant Fixed
6    Non-Participant Fixed
7    Normal          Fixed
8    Normal          Fixed
9    Normal          Fixed
10   Normal          Fixed
17   Normal          Normal
               :
               :
23   Normal          Normal
24   Normal          Normal
```

set applicant

Syntax:
set applicant <range> <normal|non-participant>
Description:
To set default applicant mode for each port.
Argument:
<range>: port range, syntax 1,5-7, available from 1 to 24
<normal>: set applicant as normal mode
<non-participant>: set applicant as non-participant mode
Possible value:
<range>: 1 to 24
<normal|non-participant>: normal or non-participant
Example:
SNMP-GSH2416(gvrp)# set applicant 1-10 non-participant

set registrar

Syntax:
set registrar <range> <normal|fixed|forbidden>
Description:
To set default registrar mode for each port.
Argument:
<range>: port range, syntax 1,5-7, available from 1 to 24
<normal>: set registrar as normal mode
<fixed>: set registrar as fixed mode
<forbidden>: set registrar as forbidden mode
Possible value:
<range>: 1 to 24
<normal|fixed|forbidden>: normal or fixed or forbidden
Example:
SNMP-GSH2416(gvrp)# set registrar 1-5 fixed

set restricted

Syntax:
set restricted <range> <enable|disable>
Description:
To set the restricted mode for each port.
Argument:
<range>: port range, syntax 1,5-7, available from 1 to 24
<enable>: set restricted enabled
<disable>: set restricted disabled
Possible value:
<range>: 1 to 24
<enable|disable>: enable or disable
Example:

```
SNMP-GSH2416(gvrp)# set restricted 1-10 enable
SNMP-GSH2416(gvrp)# show config
GVRP state: Enable
Port Join Time Leave Time LeaveAll Time    Applicant    Registrar Restricted
---- --------- ---------- ------------- ---------------- --------- ----------
  1       20         60         1000      Normal           Normal      Enable
  2       20         60         1000      Normal           Normal      Enable
  3       20         60         1000      Normal           Normal      Enable
  4       20         60         1000      Normal           Normal      Enable
  5       20         60         1000      Normal           Normal      Enable
  6       20         60         1000      Normal           Normal      Enable
  7       20         60         1000      Normal           Normal      Enable
  8       20         60         1000      Normal           Normal      Enable
  9       20         60         1000      Normal           Normal      Enable
 10       20         60         1000      Normal           Normal      Enable
                                             :
                                             :
                                             :
 22       20         60         1000      Normal           Normal      Disable
 23       20         60         1000      Normal           Normal      Disable
 24       20         60         1000      Normal           Normal      Disable
```

set timer

Syntax:
set timer <range> <join> <leave> <leaveall>
Description:
To set gvrp join time, leave time, and leaveall time for each port.
Argument:
<range> : port range, syntax 1,5-7, available from 1 to 24
<join>: join timer, available from 20 to 100
<leave>: leave timer, available from 60 to 300
<leaveall>: leaveall timer, available from 1000 to 5000
Leave Time must equal double Join Time at least.
Possible value:
<range> : 1 to 24
<join>: 20 to 100
<leave>: 60 to 300
<leaveall>: 1000 to 5000
Example:
SNMP-GSH2416(gvrp)# set timer 2-8 25 80 2000

show config

Syntax:
show config
Description:
To display the gvrp configuration.
Argument:
None.
Possible value:
None.
Example:

```
SNMP-GSH2416(gvrp)# show config
GVRP state: Enable
Port Join Time Leave Time LeaveAll Time    Applicant    Registrar Restricted
---- --------- ---------- ------------- ---------------- --------- ----------
  1       20         60          1000      Normal          Normal      Disable
  2       25         80          2000      Normal          Normal      Disable
  3       25         80          2000      Normal          Normal      Disable
  4       25         80          2000      Normal          Normal      Disable
  5       25         80          2000      Normal          Normal      Disable
  6       25         80          2000      Normal          Normal      Disable
  7       25         80          2000      Normal          Normal      Disable
  8       25         80          2000      Normal          Normal      Disable
                                             :
                                             :
 23       20         60          1000      Normal          Normal      Disable
 24       20         60          1000      Normal          Normal      Disable
```

show counter

Syntax:
show counter <port>
Description:
To display the counter number of the port.
Argument:
<port>: port number
Possible value:
<port>: available from 1 to 24
Example:

```
SNMP-GSH2416(gvrp)# show counter 2
GVRP Counter port: 2
Counter Name           Received Transmitted
--------------------   -------- -----------
Total GVRP Packets            0           0
Invalid GVRP Packets          0        ----
LeaveAll message              0           0
JoinEmpty message             0           0
JoinIn message                0           0
LeaveEmpty message            0           0
Empty message                 0           0
```

show group

Syntax:
show group
Description:
To show the gvrp group.
Argument:
None.
Possible value:
None.
Example:

```
SNMP-GSH2416(gvrp)# show group
GVRP group information
VID  Member Port
---- ------------------------------------------------
```

■ hostname

hostname

Syntax:
hostname <name>
Description:
To set up the hostname of the switch.
Argument:
<name>: hostname, max. 40 characters.
Possible value:
<name>: hostname, max. 40 characters.
Example:
SNMP-GSH2416# hostname Company

Company#

■ igmp-snooping

add allowed-group

Syntax:
add allowed-group <ip-multicast> <vid> <port-range>
Description:
To add the entry of allowed IP multicast group.
Argument:
<ip-multicast>: the range of IP multicast.
<vid>: vlan ID. 0-4094 or any. “0” value means tag-based vlan disable
<port-range>: syntax 1,5-7, available from 1 to 24
Possible value:
<ip-multicast>: ex: 224.1.1.1-225.2.3.3 or any
<vid>: 0-4094 or any
<port-range>: 1 to 24
Example:
SNMP-GSH2416(igmp-snooping)# add allowed-group 224.1.1.1-225.2.3.3 100 1-10

del allowed-group

Syntax:
del allowed-group <index>
Description:
To remove the entry of allowed ip multicast group
Argument:
<index>: the index of the allowed-group.
Possible value:
<index>: the index of the allowed-group.
Example:
SNMP-GSH2416(igmp-snooping)# del allowed-group 1

set mode

Syntax:
set mode <status>
Description:
To set up the mode of IGMP Snooping.
Argument:
<status>: 0:disable, 1:active, 2:passive
Possible value:
<status>: 0,1or 2
Example:
SNMP-GSH2416(igmp-snooping)# set mode 2

show igmp-snooping

Syntax:
show igmp-snooping
Description:
To display IGMP snooping mode and allowed IP multicast entry.
Argument:
None.
Possible value:
None.
Example:
SNMP-GSH2416(igmp-snooping)# show igmp-snooping
Snoop Mode: Active

IP Multicast:
1) IP Address : 224.1.1.1
VLAN ID : 0
Member Port : 22

show multicast

Syntax:
show multicast
Description:
To display IP multicast table.
Argument:
None.
Possible value:
None.
Example:
SNMP-GSH2416(igmp-snooping)# show multicast
IP Multicast: None

■ **IP**

disable dhcp

Syntax:
disable dhcp
Description:
To disable the DHCP function of the system.
Argument:
None.
Possible value:
None.
Example:
SNMP-GSH2416(ip)# disable dhcp

enable dhcp

Syntax:
enable dhcp <manual|auto>
Description:
To enable the system DHCP function and set DNS server via manual or auto mode.
Argument:
<manual|auto> : set dhcp by using manual or auto mode.
Possible value:
<manual|auto> : manual or auto
Example:
SNMP-GSH2416(ip)# enable dhcp manual

set dns

Syntax:
set dns <ip>
Description:
To set the IP address of DNS server.
Argument:
<ip> : dns ip address
Possible value:
168.95.1.1
Example:
SNMP-GSH2416 (ip)# set dns 168.95.1.1

set ip

Syntax:
set ip <ip> <mask> <gateway>
Description:
To set the system IP address, subnet mask and gateway.
Argument:
<ip> : ip address
<mask> : subnet mask
<gateway> : default gateway
Possible value:
<ip> : 192.168.1.2 or others
<mask> : 255.255.255.0 or others
<gateway> : 192.168.1.253 or others
Example:
SNMP-GSH2416(ip)# set ip 192.168.1.2 255.255.255.0 192.168.1.253

show

Syntax:
show
Description:
To display the system's DHCP function state, IP address, subnet mask, default gateway, DNS mode, DNS server IP address and current IP address.
Argument:
None.
Possible value:
None.
Example:

```
SNMP-GSH2416(ip)# show

DHCP               : Disable
IP Address         : 192.168.2.237
Current IP Address : 192.168.2.237
Subnet mask        : 255.255.255.0
Gateway            : 192.168.2.252
DNS Setting        : Manual
DNS Server         : 168.95.1.1
```

■ log

clear

Syntax:
clear
Description:
To clear the log data.
Argument:
None.
Possible value:
None.
Example:
SNMP-GSH2416(log)# clear

disable auto-upload

Syntax:
disable auto-upload
Description:
To disable the auto-upload function.
Argument:
None.
Possible value:
None.
Example:
SNMP-GSH2416(log)# disable auto-upload

enable auto-upload

Syntax:
enable auto-upload
Description:
To enable the auto-upload function.
Argument:
None.
Possible value:
None.
Example:
SNMP-GSH2416(log)# enable auto-upload

show

Syntax:
show
Description:
To show a list of trap log events. When any of log events happens, it will be recorded and using show command in log function to query. Up to 120 log records are supported.
Argument:
None.
Possible value:
None.
Example:

```
SNMP-GSH2416(log)# show

Tftp Server : 0.0.0.0
Auto Upload : Disable

1)  Wed Apr 13 12:13:27 2005  Link Up [Port 1]
2)  Wed Apr 13 12:13:26 2005  Link Down [Port 1]
3)  Wed Apr 13 11:58:31 2005  Login [admin]
4)  Wed Apr 13 11:19:45 2005  Login [admin]
5)  Wed Apr 13 11:19:37 2005  Logout [admin]
```

upload

Syntax:
upload
Description:
To upload log data through tftp.
Argument:
None.
Possible value:
None.
Example:
SNMP-GSH2416(log)# upload

■ mac-table

<<alias>>

del

Syntax:
del <mac>
Description:
To delete the mac alias entry.
Argument:
<mac> : mac address, format: 00-02-03-04-05-06
Possible value:
<mac> : mac address
Example:
SNMP-GSH2416(mac-table-alias)# del 00-44-33-44-55-44

set

Syntax:
set <mac> <alias>
Description:
To set up the mac alias entry.
Argument:
<mac> : mac address, format: 00-02-03-04-05-06
<alias> : mac alias name, max. 15 characters
Possible value:
None.
Example:
SNMP-GSH2416(mac-table-alias)# set 00-44-33-44-55-44 www

show

Syntax:
show
Description:
To display the mac alias entry.
Argument:
None.
Possible value:
None.
Example:
SNMP-GSH2416(mac-table-alias)# show
MAC Alias List

	MAC Address	Alias
1)	00-02-03-04-05-06	aaa
2)	00-33-03-04-05-06	ccc
3)	00-44-33-44-55-44	www

<<information>>

search

Syntax:
search <port> <mac> <vid>
Description:
To look for the relative mac information in mac table.
Argument:
<port> : set up the range of the ports to search for,
syntax 1,5-7, available form 1 to 24
<mac> : mac address, format: 01-02-03-04-05-06, '?' can be used
<vid> : vlan id, from 1 to 4094; '?' as don't care, 0 as untagged
Possible value:
<port> :1 to 24
<vid> : 0, 1 ~4094
Example:

```
SNMP-GSH2416(mac-table-information)# search 1-24 ??-??-??-??-??-?? ?
MAC Table List
Alias            MAC Address       Port VID  State
---------------- ----------------- ---- ---- -----------------
                 00-40-c7-88-00-06    1   0  Dynamic
```

show

Syntax:
show
Description:
To display all mac table information.
Argument:
None.
Possible value:
None.
Example:

```
SNMP-GSH2416 (mac-table-information)# show
MAC Table List
Alias            MAC Address       Port VID  State
---------------- ----------------- ---- ---- -----------------
                 00-10-db-1d-c5-a0   16    0 Dynamic
                 00-40-f4-89-c9-7f   16    0 Dynamic
                 00-e0-18-2b-9d-e2   16    0 Dynamic
                 00-40-c7-d8-00-02   16    0 Dynamic
```

<<maintain>>

set aging

Syntax:
set aging <#>
Description:
To set up the age out time of dynamic learning mac.
Argument:
<#>: age-timer in seconds, 0, 10 to 65535. The value “0” means to disable aging
Possible value:
<#>: 0, 10 to 65535.
Example:
SNMP-GSH2416(mac-table-maintain)# set aging 300

set flush

Syntax:
set flush
Description:
To delete all of the MACs that is learned dynamically.
Argument:
None.
Possible value:
None.
Example:
SNMP-GSH2416(mac-table-maintain)# set flush

show

Syntax:
show
Description:
To display the settings of age-timer.
Argument:
None.
Possible value:
None.
Example:
SNMP-GSH2416(mac-table-maintain)# show
age-timer : 300 seconds
SNMP-GSH2416(mac-table-maintain)#

<<static-mac>>

add

Syntax:
add <mac> <port> <vid> [alias]
Description:
To add the static mac entry.
Argument:
<mac> : mac address, format: 00-02-03-04-05-06
<port> : 0-24. The value “0” means this entry is filtering entry
<vid> : vlan id. 0, 1-4094. VID must be zero if vlan mode is not tag-based
[alias] : mac alias name, max. 15 characters
Possible value:
<mac> : mac address
<port> : 0-24
<vid> : 0, 1-4094
[alias] : mac alias name
Example:
SNMP-GSH2416(mac-table-static-mac)# add 00-02-03-04-05-06 3 0 aaa

del

Syntax:
del <mac> <vid>
Description:
To remove the static mac entry.
Argument:
<mac> : mac address, format: 00-02-03-04-05-06
<vid> : vlan id. 0, 1-4094. VID must be zero if vlan mode is not tag-based
Possible value:
<mac> : mac address
<vid> : 0, 1-4094
Example:
SNMP-GSH2416(mac-table-static-mac)# del 00-02-03-04-05-06 0

show filter

Syntax:
show filter
Description:
To display the static filter table.
Argument:
None.
Possible value:
None.
Example:
SNMP-GSH2416(mac-table-static-mac)# show filter
Static Filtering Etnry: (Total 1 item(s))
1) mac: 00-33-03-04-05-06, vid: -, alias: ccc

show forward

Syntax:
show forward
Description:
To display the static forward table.
Argument:
None.
Possible value:
None.
Example:
SNMP-GSH2416(mac-table-static-mac)# show forward
Static Forwarding Etnry: (Total 1 item(s))
1) mac: 00-02-03-04-05-06, port: 3, vid: -, alias: aaa

■ management

add

Syntax:
Usage: set [<name> <value>] [<vid> <value>] [<ip> <value>] [<port> <value>] [<type> <value>] <action> <value>
Synopsis: set name Mary vid 20 ip 192.168.1.1-192.168.1.90 port 2-5,8 type h,s action a
Synopsis: set name Mary vid 20 ip 192.168.1.1-192.168.1.90
Description:
To save the adding management policy records.
When you don't know how to set the management policy records, you can use this command as follows:
SNMP-GSH2416 (management-add)# set
This command will show exhaustive operating explanation for setting the management policy records.
Argument:

[<name> <value>]	ACL entry name.
[<vid> <value>]	VLAN ID.
[<ip> <value>]	IP range.
[<port> <value>]	Incoming port.
[<type> <value>]	Access type.
<action> <value>	a(ccept) or d(eny).

Possible value:

[<name> <value>]	No default and it must be set.
[<vid> <value>]	The range is 1-4095 and can be set to any.
[<ip> <value>]	For example, 192.168.1.90-192.168.1.90 or any.
[<port> <value>]	For example, 1 or 1-8 or 1,3-5 or any
[<type> <value>]	For example, h(ttp),s(nmp),t(elnet) or any.
<action> <value>	No default and it must be set.

Example:

```
SNMP-GSH2416(management-add)# set name Mary vid 20 ip 192.168.1.1-
192.168.1.90 port 2-5,8 type h,s action a


SNMP-GSH2416(management-add)# show

 #: 1
Name : Mary              VlanID : 20        IP : 192.168.1.1-192.168.1.90
Type : Http,SNMP         Action : Accept    Port : 2,3,4,5,8
```

delete

Syntax:
delete #
Description:
To delete a specific record or range.
Argument:
<#>: a specific or range management security entry(s)
Possible value:
None.
Example:

```
SNMP-GSH2416(management)# show

 #: 1
Name : Tom                VlanID : 2         IP : 192.168.1.30-192.168.1.80
Type : SNMP               Action : Deny      Port : 1,2

SNMP-GSH2416(management)# delete 1

SNMP-GSH2416(management)# show

Security rule list is empty now
```

edit [#]: the specific management policy entry. Available range: 1 to 65536.

Syntax:

Usage: set [<name> <value>] [<vid> <value>] [<ip> <value>] [<port> <value>]
[<type> <value>] <action> <value>

Synopsis: set name Mary vid 20 ip 192.168.1.1-192.168.1.90 port 2-5,8
type h,s action a

Synopsis: set name Mary vid 20 ip 192.168.1.1-192.168.1.90

Description:

To edit management policy record.

Argument:

[<name> <value>]	ACL entry name.
[<vid> <value>]	VLAN ID.
[<ip> <value>]	IP Range.
[<port> <value>]	Incoming port.
[<type> <value>]	Access type.
<action> <value>	a(ccept) or d(eny).

Possible value:

[<name> <value>]	No default and it must be set.
[<vid> <value>]	The range is 1-4095 and can be set to any.
[<ip> <value>]	For example, 192.168.1.90-192.168.1.90 or any
[<port> <value>]	For example, 1 or 1-8 or 1,3-5 or any
[<type> <value>]	For example, h(ttp),s(nmp),t(elnet) or any
<action> <value>	No default and it must be set.

Example:

```
SNMP-GSH2416(management)# edit 1

SNMP-GSH2416(management-edit-1)# set name Tom vid 2 ip 192.168.1.30-
                                 192.168.1.80 port 1-2 type s action d
SNMP-GSH2416(management-edit-1)# show

 #: 1
Name : Tom                VlanID : 2          IP : 192.168.1.30-192.168.1.80
Type : SNMP               Action : Deny       Port : 1,2
```

show

Syntax:
show
Description:
To show the specific management policy record.
Argument:
None.
Possible value:
None.
Example:

```
SNMP-GSH2416(management)# show

 #: 1
Name : Tom                VlanID : 2          IP : 192.168.1.30-192.168.1.80
Type : SNMP               Action : Deny       Port : 1,2
```

■ max-pkt-len

set len

Syntax:
set len <range> <length>
Description:
To set up the maximum length of the packet that each port of the switch can accept.
Argument:
<range>: port range, syntax 1,5-7, available from 1 to 24
<length (bytes)>: maximum packet length
Possible value:
<range> : 1 to 24
<length (bytes)>: 1518/1532/9216
Example:
SNMP-GSH2416(max-pkt-len)# set len 1-8 9216

show

Syntax:
show
Description:
To show current setting of maximum packet length setting.
Argument:
None.
Possible value:
None.
Example:
SNMP-GSH2416(max-pkt-len)# show

PORT	Max Packet Length
1	1532
2	1532
3	1532
4	1532
5	1532
6	1532
7	1532
8	1532
9	1532
10	1532
11	1532
12	1532
13	1532
14	1532
15	1532
16	1532
17	1532
18	1532
19	1532
20	1532
21	1532
22	1532
23	1532
24	1532

■ mirror

set mirror-mode

Syntax:
set mirror-mode <rx|disable>
Description:
To set up the mode of mirror (rx mode or disable).
Argument:
<rx | disable>:
rx : enable the mode of mirror(Only mirror the packets that is received)
disable: end the function of mirror
Possible value:
<rx | disable>: rx or disable
Example:
SNMP-GSH2416(mirror)# set mirror-mode rx

set monitored-port

Syntax:
set monitored-port <range>
Description:
To set up the port that will be monitored. The packets received by this port will be copied to the monitoring port.
Argument:
<range>: the port that is chosen for monitored port of the mirror function, syntax 1,5-7, available from 1 to 24
Possible value:
<range>: 1 to 24
Example:
SNMP-GSH2416(mirror)# set monitored-port 3-5,8,10

set monitoring-port

Syntax:
set monitoring-port <#>
Description:
To set up the monitoring port of the mirror function. User can observe the packets that the monitored port received via this port.
Argument:
<#>: the monitoring port that is chosen for the mirror function. Only one port is allowed to configure, available from 1 to 24
Possible value:
<#>:1 to 24
Example:
SNMP-GSH2416(mirror)# set monitoring-port 2

show

Syntax:
show
Description:
To display the setting status of Mirror function.
Argument:
None.
Possible value:
None.
Example:
SNMP-GSH2416(mirror)# show
Mirror Mode : rx
Monitoring Port : 2
Monitored Port : 3 4 5 7 10

■ port

clear counter

Syntax:
clear counter
Description:
To clear all ports' counter (include simple and detail port counter) information.
Argument:
None.
Possible value:
None.
Example:
SNMP-GSH2416 (port)# clear counter

disable flow-control

Syntax:
disable flow-control <range>
Description:
To disable the flow control function of the port.
Argument:
<range>: syntax 1,5-7, available from 1 to 24
Possible value:
<range>: 1 ~ 24
Example:
SNMP-GSH2416 (port)# disable flow-control 6

disable state

Syntax:
disable state <range>
Description:
To disable the communication capability of the port.
Argument:
<range>: syntax 1,5-7, available from 1 to 24
Possible value:
<range>: 1 ~ 24
Example:
SNMP-GSH2416 (port)# disable state 12

enable flow-control

Syntax:
enable flow-control <range>
Description:
To enable the flow control function of the port.
Argument:
<range>: syntax 1,5-7, available from 1 to 24
Possible value:
<range>: 1 ~ 24
Example:
SNMP-GSH2416 (port)# enable flow-control 3-8

enable state

Syntax:
enable state <range>
Description:
To enable the communication capability of the port.
Argument:
<range>: syntax 1,5-7, available from 1 to 24
Possible value:
<range>: 1 ~ 24
Example:
SNMP-GSH2416 (port)# enable state 3-12

set speed-duplex

Syntax:
set speed-duplex <range> <auto|10half|10full|100half|100full|1Gfull>
Description:
To set up the speed and duplex of all ports.
Argument:
<range>:syntax 1,5-7, available from 1 to 24
<port-speed>:
auto: set auto-negotiation mode
10half: set speed/duplex 10M Half
10full: set speed/duplex 10M Full
100half: set speed/duplex 100M Half
100full: set speed/duplex 100M Full
1Gfull: set speed/duplex 1G Full
Possible value:
<range>: 1 to 24
<port-speed>: auto, 10half, 10full, 100half, 100full, 1Gfull
Example:
SNMP-GSH2416(port)# set speed-duplex 5 auto

show conf

Syntax:
show conf
Description:
To display the each port's configuration about state, speed-duplex and flow control.
Argument:
None.
Possible value:
None.
Example:
SNMP-GSH2416 (port)# show conf

show detail-counter

Syntax:
show detail-counter <#>
Description:
To display the detailed counting number of each port's traffic.
Argument:
<#>: port, available from 1 to 24
Possible value:
<#>:1 ~ 24
Example:
SNMP-GSH2416 (port)# show detail-counter 5

show sfp

Syntax:
show sfp <port>
Description:
To display the SFP module information.
Argument:
<port>: SFP port of the switch, available from 9 to 24
Possible value:
<port>: 9 to 24
Example:
SNMP-GSH2416 (port)# show sfp 9

```
Port 9 SFP information
------------------------------------------------------------------------
Connector Type        : SFP - LC
Fiber Type            : Multi-mode (MM)
Tx Central Wavelength : 850
Baud Rate             : 1G
Vendor OUI            : 00:40:c7
Vendor Name           : APAC Opto
Vendor PN             : KM28-C3S-TC-N
Vendor Rev            : 0000
Vendor SN             : 5425010728
Date Code             : 050530
Temperature           : none
Vcc                   : none
Mon1 (Bias) mA        : none
Mon2 (TX PWR)         : none
Mon3 (RX PWR)         : none
```

show simple-counter

Syntax:
show simple-counter
Description:
To display the summary counting of each port's traffic.
Argument:
None.
Possible value:
None.
Example:
SNMP-GSH2416 (port)# show simple-counter

show status

Syntax:
show status
Description:
To display the port's current status.
Argument:
None.
Possible value:
None.
Example:
SNMP-GSH2416 (port)# show status

■ qos

set advance-layer4

Syntax:
set advance-layer4 <port-range> <#> <tcp/udp port> <default> <match>
Description:
To set class of ports on advanced mode of Layer 4 qos.
Argument:
<port-range>: port range, syntax 1,5-7, available from 1 to 24
<#>: special UDP/TCP port selection, range: 1-10
<tcp/udp port range>: 0-65535.
<default>: default class (all other TCP/UDP ports). 1: high, 0: low
<match>: special TCP/UDP class. 1: high, 0: low
Possible value:
<port-range>: 1 to 24
<#>: 1-10
<tcp/udp port range>: 0-65535
<default>: 1 or 0
<match>: 1 or 0
Example:
SNMP-GSH2416(qos)# set advance-layer4 5 2 80 1 0

set default

Syntax:
set default <class>
Description:
To set priority class of the packets that qos won't affect.
Argument:
<class>: class of service setting. 1: high, 0: low
Possible value:
<class>: 1 or 0
Example:
SNMP-GSH2416(qos)# set default 1

set diffserv

Syntax:
set diffserv <ds-range> <class>
Description:
To set class of ports on IP DiffServe qos.
Argument:
<ds-range>: dscp field, syntax 1,5-7, available from 0 to 63
<class>: class of service setting. 1: high, 0: low
Possible value:
<ds-range>: 0 to 63
<class>: 1or 0
Example:
SNMP-GSH2416(qos)# set diffserv 0-20 1

set mode

Syntax:
set mode <port/pri_tag/tos/layer4/diffserv>
Description:
To set qos priority mode of the switch.
Argument:
<port>: per port priority
<pri_tag>: vlan tag priority
<tos>: ip tos classification
<layer4>: ip tcp/udp port classification
<diffserv>: ip diffserv classification
Possible value:
port/pri_tag/tos/layer4/diffserv
Example:
SNMP-GSH2416(qos)# set mode port

set port

Syntax:
set port <range> <class>
Description:
To set class of ports on port-based qos.
Argument:
<range> : port range, syntax 1,5-7, available from 1 to 24
<class> : class of service setting. 1: high, 0: low
Possible value:
<range>: 1 to 24
<class>: 1or 0
Example:
SNMP-GSH2416(qos)# set port 1-10 1

set pri-tag

Syntax:
set pri_tag <port-range> <tag-range> <class>
Description:
To set class of ports on vlan tag-based qos.
Argument:
<port-range>: port range, syntax 1,5-7, available from 1 to 24
<tag-range>: tag priority level, syntax: 1,5-7, available from 0 to 7
<class>: class of service setting. 1: high, 0: low
Possible value:
<port-range>: 1 to 24
<tag-range>: 0 to 7
<class>: 1or 0
Example:
```
SNMP-GSH2416(qos)# set pri-tag 1-15 1-2 1
```

set simple-layer4

Syntax:
set simple-layer4 <#>
Description:
To set class of ports on simple mode of Layer 4 qos.
Argument:
<#>: layer-4 configuration mode, valid values are as follows:
0: disable ip tcp/udp port classification
1: down prioritize web browsing, e-mail, FTP and news
2: prioritize ip telephony (VoIP)
3: prioritize iSCSI
4: prioritize web browsing, e-mail, FTP transfers and news
5: prioritize streaming Audio/Video
6: prioritize databases (Oracle, IBM DB2, SQL, Microsoft)
Possible value:
<#>:0~6
Example:
SNMP-GSH2416(qos)# set simple-layer4 2

set tos

Syntax:
set tos <port-range> <tos-range> <class>
Description:
To set class of ports on IP TOS qos.
Argument:
<port-range>: port range, syntax: 1,5-7, available from 1 to 24
<tos-range>: tos precedence field, syntax 1,5-7, available from 0 to 7
<class>: class of service setting. 1: high, 0: low
Possible value:
<port-range>: 1 to 24
<tos-range>: 0 to 7
<class>: 1or 0
Example:

```
SNMP-GSH2416(qos)# set tos 1-5 0-3 0
```

show

Syntax:
show
Description:
To display the information of the mode you choose.
Argument:
None.
Possible value:
None.
Example:

```
SNMP-GSH2416 (qos)# show
IP Diffserv Classification

Default Class:high

 DiffServ   Class   DiffServ   Class   DiffServ   Class   DiffServ   Class
---------- ------- ---------- ------- ---------- ------- ---------- -------
     0      high        1      high        2      high        3      high
     4      high        5      high        6      high        7      high
     8      high        9      high       10      high       11      high
    12      high       13      high       14      high       15      high
    16      high       17      high       18      high       19      high
    20      high       21      high       22      high       23      high
    24      high       25      high       26      high       27      high
    28      high       29      high       30      high       31      high
    32      high       33      high       34      high       35      high
    36      high       37      high       38      high       39      high
    40      high       41      high       42      high       43      high
    44      high       45      high       46      high       47      high
    48      high       49      high       50      high       51      high
    52      high       53      high       54      high       55      high
    56      high       57      high       58      high       59      high
    60      high       61      high       62      high       63      high
```

■ reboot

reboot

Syntax:
reboot
Description:
To reboot the system.
Argument:
None.
Possible value:
None.
Example:
SNMP-GSH2416# reboot

■ snmp

disable

Syntax:
disable set-ability
disable snmp
Description:
The Disable here is used for the de-activation of snmp or set-community.
Argument:
None.
Possible value:
None.
Example:
```
SNMP-GSH2416(snmp)# disable snmp
SNMP-GSH2416(snmp)# disable set-ability
```

enable

Syntax:
enable set-ability
enable snmp
Description:
The Enable here is used for the activation snmp or set-community.
Argument:
None.
Possible value:
None.
Example:
```
SNMP-GSH2416(snmp)# enable snmp
SNMP-GSH2416(snmp)# enable set-ability
```

set

Syntax:
set get-community <community>
set set-community <community>
set trap <#> <ip> [port] [community]
Description:
The Set here is used for the setup of get-community, set-community, trap host ip, host port and trap-community.
Argument:
<#>: trap number
<ip>: ip address or domain name
<port>: trap port
<community>:trap community name
Possible value:
<#>: 1 to 6
<port>:1~65535
Example:

```
SNMP-GSH2416(snmp)# set get-community public
SNMP-GSH2416(snmp)# set set-community private
SNMP-GSH2416(snmp)# set trap 1 192.168.1.1 162 public
```

show

Syntax:
show
Description:
The Show here is to display the configuration of SNMP.
Argument:
None.
Possible value:
None.
Example:

```
SNMP-GSH2416(snmp)# show
SNMP          : Enable
Get Community: public
Set Community: private [Enable]
Trap Host 1 IP Address: 192.168.1.1 Port: 162 Community: public
Trap Host 2 IP Address: 0.0.0.0 Port: 162 Community: public
Trap Host 3 IP Address: 0.0.0.0 Port: 162 Community: public
Trap Host 4 IP Address: 0.0.0.0 Port: 162 Community: public
Trap Host 5 IP Address: 0.0.0.0 Port: 162 Community: public
Trap Host 6 IP Address: 0.0.0.0 Port: 162 Community: public
```

■ **stp**

MCheck

Syntax:
MCheck <range>
Description:
To force the port to transmit RST BPDUs.
Argument:
<range>: syntax 1,5-7, available from 1 to 24
Possible value:
<range>: 1 to 24
Example:
SNMP-GSH2416(stp)# Mcheck 1-8

disable

Syntax:
disable
Description:
To disable the STP function.
Argument:
None.
Possible value:
None.
Example:
SNMP-GSH2416(stp)# disable

enable

Syntax:
enable
Description:
To enable the STP function.
Argument:
None.
Possible value:
None.
Example:
SNMP-GSH2416(stp)# enable

set config

Syntax:
set config <Bridge Priority> <Hello Time> <Max. Age> <Forward Delay>
Description:
To set up the parameters of STP.
Argument:
<Bridge Priority>:priority must be a multiple of 4096, available from 0 to 61440.
<Hello Time>: available from 1 to 10.
<Max. Age>: available from 6 to 40.
<Forward Delay>: available from 4 to 30.
Note: 2*(Forward Delay -1) >= Max Age
Max Age >= 2*(Hello Time +1)
Possible value:
<Bridge Priority>: 0 to 61440
<Hello Time>: 1 to 10
<Max. Age>: 6 to 40
<Forward Delay>: 4 to 30
Example:
SNMP-GSH2416(stp)# set config 61440 2 20 15

set port

Syntax:
set port <range> <path cost> <priority> <edge_port> <admin p2p>
Description:
To set up the port information of STP.
Argument:
<range>: syntax 1,5-7, available from 1 to 24
<path cost>: 0, 1-200000000. The value zero means auto status
<priority>: priority must be a multiple of 16, available from 0 to 240
<edge_port> : Admin Edge Port, <yes|no>
<admin p2p>: Admin point to point, <auto|true|false>
Possible value:
<range>:1 to 24
<path cost>: 0, 1-200000000
<priority>: 0 to 240
<edge_port>: yes / no
<admin p2p>: auto / true / false
Example:
SNMP-GSH2416(stp)# set port 1-16 0 128 yes auto

set version

Syntax:
set version <stp|rstp>
Description:
To set up the version of STP.
Argument:
<stp|rstp>:stp / rstp
Possible value:
<stp|rstp>:stp / rstp
Example:
SNMP-GSH2416(stp)# set version rstp

show config

Syntax:
show config
Description:
To display the configuration of STP.
Argument:
None.
Possible value:
None.
Example:

```
SNMP-GSH2416(stp)# show config
STP State Configuration    :
Spanning Tree Protocol     : Enabled
Bridge Priority (0-61440)  : 61440
Hello Time (1-10 sec)      : 2
Max. Age (6-40 sec)        : 20
Forward Delay (4-30 sec)   : 15
Force Version              : RSTP
```

show port

Syntax:
show port
Description:
To display the port information of STP.
Argument:
None.
Possible value:
None.
Example:

```
SNMP-GSH2416# stp
SNMP-GSH2416(stp)# show port
Port Port Status Path Cost Priority Admin Edge Port Admin Point To Point
==== =========== ========= ======== ================ ====================
  1  DISCARDING    2000000    128         No                Auto
  2  DISCARDING    2000000    128         No                Auto
  3  DISCARDING    2000000    128         No                Auto
  4  DISCARDING    2000000    128         No                Auto
  5  DISCARDING    2000000    128         No                Auto
  6  DISCARDING    2000000    128         No                Auto
  7  DISCARDING    2000000    128         No                Auto
  8  DISCARDING    2000000    128         No                Auto
  9  DISCARDING    2000000    128         No                Auto
 10  DISCARDING    2000000    128         No                Auto
 11  DISCARDING    2000000    128         No                Auto
 12  DISCARDING    2000000    128         No                Auto
 13  DISCARDING    2000000    128         No                Auto
 14  DISCARDING    2000000    128         No                Auto
 15  DISCARDING    2000000    128         No                Auto
 16  DISCARDING    2000000    128         No                Auto
 17  DISCARDING    2000000    128         No                Auto
 18  DISCARDING    2000000    128         No                Auto
 19  DISCARDING    2000000    128         No                Auto
 20  DISCARDING    2000000    128         No                Auto
 21  DISCARDING    2000000    128         No                Auto
 22  DISCARDING    2000000    128         No                Auto
...(q to quit)

 23  DISCARDING    2000000    128         No                Auto
 24  DISCARDING    2000000    128         No                Auto
```

show status

Syntax:
show status
Description:
To display the status of STP.
Argument:
None.
Possible value:
None.
Example:
SNMP-GSH2416(stp)# show status

```
STP Status :
STP State                          : Enabled
Bridge ID                          : 00:40:C7:D8:09:1D
Bridge Priority                    : 61440
Designated Root                    : 00:40:C7:D8:09:1D
Designated Priority                : 61440
Root Port                          : 0
Root Path Cost                     : 0
Current Max. Age(sec)              : 20
Current Forward Delay(sec)         : 15
Hello Time(sec)                    : 2
STP Topology Change Count          : 0
Time Since Last Topology Change(sec) : 848
```

■ system

set contact

Syntax:
set contact <contact string>
Description:
To set the contact description of the switch.
Argument:
<contact>:string length up to 40 characters.
Possible value:
<contact>: A, b, c, d, ... ,z and 1, 2, 3, …. etc.
Example:
SNMP-GSH2416(system)# set contact Taipei

set device-name

Syntax:
set device-name <device-name string>
Description:
To set the device name description of the switch.
Argument:
<device-name>: string length up to 40 characters.
Possible value:
<device-name>: A, b, c, d, ... ,z and 1, 2, 3, …. etc.
Example:
SNMP-GSH2416(system)# set device-name CR-2600

set location

Syntax:
set location <location string>
Description:
To set the location description of the switch.
Argument:
<location>: string length up to 40 characters.
Possible value:
<location>: A, b, c, d, ... ,z and 1, 2, 3, …. etc.
Example:
SNMP-GSH2416(system)# set location Taipei

show

Syntax:
show
Description:
To display the basic information of the switch.
Argument:
None.
Possible value:
None.
Example:

```
SNMP-GSH2416(system)# show
Model Name                     : SNMP-GSH2416
System Description             : L2 Managed Switch
Location                       :
Contact                        :
Device Name                    : SNMP-GSH2416
System Up Time                 : 0 Days 0 Hours 4 Mins 13 Secs
Current Time                   : Fri Jan 27 13:20:47 2006
BIOS Version                   : v65535.65535
Firmware Version               : v2.14
Hardware-Mechanical Version    : v65535.65535-v65535.65535
Serial Number                  : 031302000002
Host IP Address                : 192.168.1.1
Host MAC Address               : 00-aa-aa-aa-aa-aa
Device Port                    : UART * 1, TP * 8, SFP * 16
RAM Size                       : 65535 M
Flash Size                     : 65535 M
```

■ tftp

set server

Syntax:
set server <ip>
Description:
To set up the IP address of tftp server.
Argument:
<ip>: the IP address of tftp server
Possible value:
<ip>: tftp server ip
Example:
SNMP-GSH2416(tftp)# set server 192.168.3.111

show

Syntax:
show
Description:
To display the information of tftp server.
Argument:
None.
Possible value:
None.
Example:
SNMP-GSH2416(tftp)# show
Tftp Server : 192.168.3.111

■ time

set daylightsaving

Syntax:
set daylightsaving <hr> <MM/DD/HH> <mm/dd/hh>
Description:
To set up the daylight saving.
Argument:
<hr> : daylight saving hour, range: -5 to +5
<MM> : daylight saving start Month (01-12)
<DD> : daylight saving start Day (01-31)
<HH> : daylight saving start Hour (00-23)
<mm> : daylight saving end Month (01-12)
<dd> : daylight saving end Day (01-31)
<hh> : daylight saving end Hour (00-23)
Possible value:
<hr> : -5 to +5
<MM> : (01-12)
<DD> : (01-31)
<HH> : (00-23)
<mm> : (01-12)
<dd> : (01-31)
<hh> : (00-23)
Example:
SNMP-GSH2416(time)# set daylightsaving 3 10/12/01 11/12/01
Save Successfully

set manual

Syntax:
set manual <YYYY/MM/DD> <hh:mm:ss>
Description:
To set up the current time manually.
Argument:
<YYYY> : Year (2000-2036) <MM> : Month (01-12)
<DD> : Day (01-31) <hh> : Hour (00-23)
<mm> : Minute (00-59) <ss> : Second (00-59)
Possible value:
<YYYY> : (2000-2036) <MM> : (01-12)
<DD> : (01-31) <hh> : (00-23)
<mm> : (00-59) <ss> : (00-59)
Example:
SNMP-GSH2416(time)# set manual 2004/12/23 16:18:00

set ntp

Syntax:
set ntp <ip> <timezone>
Description:
To set up the current time via NTP server.
Argument:
<ip>: ntp server ip address or domain name
<timezone>: time zone (GMT), range: -12 to +13
Possible value:
<timezone>: -12,-11…,0,1…,13
Example:
SNMP-GSH2416(time)# set ntp clock.via.net 8
Synchronizing...(1)
Synchronization success

show

Syntax:
show
Description:
To show the time configuration, including “Current Time”, “NTP Server”,” Timezone”, ” Daylight Saving”,” Daylight Saving Start” and “Daylight Saving End”
Argument:
None.
Possible value:
None.
Example:

```
SNMP-GSH2416(time)# show
Current Time                : Thu Thu 14 15:04:03 2005
NTP Server                  : 209.81.9.7
Timezone                    : GMT+8:00
Day light Saving            : 0 Hours
Day light Saving Start      : Mth: 1 Day: 1 Hour: 0
Day light Saving End  : Mth: 1 Day: 1 Hour: 0
SNMP-GSH2416(time)#
```

■ trunk

del trunk

Syntax:
del trunk <port-range>
Description:
To delete the trunking port.
Argument:
<port-range>: port range, syntax 1,5-7, available from 1 to 24
Possible value:
<port-range>: 1 to 24
Example:
SNMP-GSH2416(trunk)# del trunk 1

set priority

Syntax:
set priority <range>
Description:
To set up the LACP system priority.
Argument:
<range>: available from 1 to 65535.
Possible value:
<range>: 1 to 65535, default: 32768
Example:
SNMP-GSH2416(trunk)# set priority 33333

set trunk

Syntax:
set trunk <port-range> <method> <group> <active LACP>
Description:
To set up the status of trunk, including the group number and mode of the trunk as well as LACP mode.
Argument:
<port-range> : port range, syntax 1,5-7, available from 1 to 24
<method>:
static : adopt the static link aggregation
lacp : adopt the dynamic link aggregation- link aggregation control protocol
<group>: 1-8.
<active LACP>:
active : set the LACP to active mode
passive : set the LACP to passive mode
Possible value:
<port-range> : 1 to 24
<method>: static / lacp
<group>: 1-8.
<active LACP>: active / passive
Example:
SNMP-GSH2416(trunk)# set trunk 1-4 lacp 1 active

show aggtr-view

Syntax:
show aggtr-view
Description:
To display the aggregator list.
Argument:
None.
Possible value:
None.
Example:
SNMP-GSH2416(trunk)# show aggtr-view
Aggregator 1) Method: None
Member Ports: 1
Ready Ports:1

Aggregator 2) Method: LACP
Member Ports: 2
Ready Ports:
:
:
:

show lacp-detail

Syntax:
show lacp-detail <aggtr>
Description:
To display the detailed information of the LACP trunk group.
Argument:
<aggtr>: aggregator, available from 1 to 24
Possible value:
<aggtr>: 1 to 24
Example:
SNMP-GSH2416(trunk)# show lacp-detail 2
Aggregator 2 Information:

Actor		Partner	
System Priority	MAC Address	System Priority	MAC Address
32768	00-40-c7-e8-00-02	32768	00-00-00-00-00-00

Port	Key	Trunk Status	Port	Key
2	257	---	2	0

show lacp-priority

Syntax:
show lacp-priority
Description:
To display the value of LACP Priority.
Argument:
None.
Possible value:
None.
Example:
SNMP-GSH2416(trunk)# show lacp-priority
LACP System Priority : 32768

show status

Syntax:
show status
Description:
To display the aggregator status and the settings of each port.
Argument:
None.
Possible value:
None.
Example:
SNMP-GSH2416(trunk)# show status

Trunk Port Setting				Trunk Port Status	
port	Method	Group	Active LACP	Aggtregator	Status
1	None	0	Active	1	Ready
2	LACP	1	Active	2	---
3	LACP	1	Active	3	---
4	LACP	1	Active	4	---
5	LACP	1	Active	5	---
6	LACP	1	Active	6	---
7	LACP	1	Active	7	---
			:		
			:		
19	None	0	Active	19	---
20	None	0	Active	20	---
21	None	0	Active	21	---
22	None	0	Active	22	---
23	None	0	Active	23	---
24	None	0	Active	24	---

■ vlan

del port-group

Syntax:
del port-group <name>
Description:
To delete the port-based vlan group.
Argument:
<name>: which vlan group you want to delete.
Possible value:
<name>: port-vlan name
Example:
SNMP-GSH2416(vlan)# del port-group VLAN-2

del tag-group

Syntax:
del tag-group <vid>
Description:
To delete the tag-based vlan group.
Argument:
<vid>: which vlan group you want to delete, available from 1 to 4094
Possible value:
<vid>: 1 to 4094
Example:
SNMP-GSH2416(vlan)# del tag-group 2

disable drop-untag

Syntax:
disable drop-untag <range>
Description:
Don’t drop the untagged frames.
Argument:
<range> : which port(s) you want to set, syntax 1,5-7, available from 1 to 24
Possible value:
<range>: 1 to 24
Example:
SNMP-GSH2416(vlan)# disable drop-untag 5-10

disable sym-vlan

Syntax:
disable sym-vlan <range>
Description:
To drop frames from the non-member port.
Argument:
<range>: which port(s) you want to set, syntax 1,5-7, available from 1 to 24
Possible value:
<range>: 1 to 24
Example:
SNMP-GSH2416(vlan)# disable sym-vlan 5-10

enable drop-untag

Syntax:
enable drop-untag <range>
Description:
To drop the untagged frames.
Argument:
<range>: which port(s) you want to set, syntax 1,5-7, available from 1 to 24
Possible value:
<range>: 1 to 24
Example:
SNMP-GSH2416(vlan)# enable drop-untag 5-10

enable sym-vlan

Syntax:
enable sym-vlan <range>
Description:
To drop frames from the non-member port.
Argument:
<range> : which port(s) you want to set, syntax 1,5-7, available from 1 to 24
Possible value:
<range>: 1 to 24
Example:
SNMP-GSH2416(vlan)# enable sym-vlan 5-10

set mode

Syntax:
set mode <disable|port|tag|metro|double-tag> [up-link]
Description:
To switch VLAN mode, including disable, port-based, tag-based, metro and double-tag modes.
Argument:
<disable>: vlan disable
<tag>: set tag-based vlan
<port>: set port-based vlan
<metro>: set metro mode vlan
<double-tag>: enable Q-in-Q function
<up-link>: syntax 1,5-7, available from 23 to 24, only for metro mode vlan
Possible value:
<disable|port|tag|metro|double-tag>: disable,port,tag,metro,double-tag
[up-link]: 23 or 24 or “23,24”
Example:
SNMP-GSH2416(vlan)# set mode port

set port-group

Syntax:
set port-group <name> <range>
Description:
To add or edit a port-based VLAN group.
Argument:
<name>: port-vlan name
<range>: syntax 1,5-7, available from 1 to 24
Possible value:
<range>: 1 to 24
Example:
SNMP-GSH2416(vlan)# set port-group VLAN-1 2-5,6,15-13

set port-role

Syntax:
set port-role <range> <access|trunk|hybrid> [vid]
Description:
To set egress rule: configure the port roles.
Argument:
<range> :which port(s) you want to set, syntax 1,5-7, available from 1 to 24
<access>: Do not tag frames
<trunk>: Tag all frames
<hybrid>: Tag all frames except a specific VID
<vid>: untag-vid for hybrid port
Possible value:
<range>: 1 to 24
<vid>: 1 to 4094
Example:
SNMP-GSH2416(vlan)# set port-role 5 hybrid 6

set pvid

Syntax:
set pvid <range> <pvid>
Description:
To set the pvid of vlan.
Argument:
<range>: which port(s) you want to set PVID(s), syntax 1,5-7, available from 1 to 24
<pvid>: which PVID(s) you want to set, available from 1 to 4094
Possible value:
<range>: 1 to 24
<pvid>: 1 to 4094
Example:
SNMP-GSH2416(vlan)# set pvid 3,5,6-8 5

set tag-group

Syntax:
set tag-group <vid> <name> <range> <#>
Description:
To add or edit the tag-based vlan group.
Argument:
<vid>: vlan ID, range from 1 to 4094
<name>: tag-vlan name
<range>: vlan group members, syntax 1,5-7, available from 1 to 24
<#>: sym/asym vlan setting. 1: symmetric vlan, 0: asymmetric vlan
Possible value:
<vid>: 1 to 4094
<range>: 1 to 24
<#>: 0 or 1
Example:
SNMP-GSH2416(vlan)# set tag-group 2 VLAN-2 2-5,6,15-13 0

show group

Syntax:
show group
Description:
To display the vlan mode and vlan group.
Argument:
None.
Possible value:
None.
Example:

```
SNMP-GSH2416(vlan)# show group
Vlan mode is double-tag.

1)  Vlan Name : default
    Vlan ID   : 1
    Sym-vlan  : Disable
    Member    : 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16

2)  Vlan Name : VLAN-2
    Vlan ID   : 2
    Sym-vlan  : Disable
    Member    : 2 3 4 5 6 13 14 15
```

show pvid

Syntax:
show pvid
Description:
To display pvid, ingress/egress rule.
Argument:
None.
Possible value:
None.
Example:

```
SNMP-GSH2416(vlan)# show pvid
 Port   PVID    Rule1     Rule2    Port Rule   Untag Vid
------ ------ --------- --------- ---------- ----------
   1       1   Disable   Disable     Access         -
   2       1   Disable   Disable     Access         -
   3       5   Disable   Disable     Access         -
   4       1   Disable   Disable     Access         -
   5       5   Enable    Disable     Hybrid         6
   6       5   Enable    Disable     Access         -
   7       5   Enable    Disable     Access         -
   8       5   Enable    Disable     Access         -
   9       1   Enable    Disable     Access         -
  10       1   Enable    Disable     Access         -
  11       1   Disable   Disable     Access         -
                           :
                           :
  23       1   Disable   Disable     Access         -
  24       1   Disable   Disable     Access         -
```

■ **vs**

disable

Syntax:
disable
Description:
To disable the virtual stack.
Argument:
None.
Possible value:
None.
Example:
SNMP-GSH2416(vs)# disable

enable

Syntax:
enable
Description:
To enable the virtual stack.
Argument:
None.
Possible value:
None.
Example:
SNMP-GSH2416(vs)# enable

set gid

Syntax:
set gid <gid>
Description:
To set the group id.
Argument:
<gid>:Group ID
Possible value:
<gid>:a-z,A-Z,0-9
Example:
SNMP-GSH2416(vs)# set gid group1

set role

Syntax:
set role <master|slave>
Description:
To set role.
Argument:
<master|slave>:
master: act as master, slave : act as slave
Possible value:
<master|slave>: master or slave
Example:

```
SNMP-GSH2416(vs)# set role master
```

show

Syntax:
show
Description:
To display the configuration of the virtual stack.
Argument:
None.
Possible value:
None.
Example:

```
SNMP-GSH2416(vs)# show
Virtual Stack Config:
State     : Enable
Role      : Master
Group ID  : group1
```

5. Maintenance

5-1. Resolving No Link Condition

The possible causes for a no link LED status are as follows:

- The attached device is not powered on
- The cable may not be the correct type or is faulty
- The installed building premise cable is faulty
- The port may be faulty

5-2. Q&A

1. Computer A can connect to Computer B, but cannot connect to Computer C through the Managed Switch.
   - ✓ The network device of Computer C may fail to work. Please check the link/act status of Computer C on the LED indicator. Try another network device on this connection.
   - ✓ The network configuration of Computer C may be something wrong. Please verify the network configuration on Computer C.

2. The uplink connection function fails to work.
   - ✓ The connection ports on another must be connection ports. Please check if connection ports are used on that Managed Switch.
   - ✓ Please check the uplink setup of the Managed Switch to verify the uplink function is enabled.

3. The console interface cannot appear on the console port connection.
   - ✓ The COM port default parameters are [Baud Rate: 57600, Data Bits: 8, Parity Bits: None, Stop Bit: A, Flow Control: None]. Please check the COM port property in the terminal program. And if the parameters are changed, please set the COM configuration to the new setting.
   - ✓ Check the RS-232 cable is connected well on the console port of the Managed Switch and COM port of PC.
   - ✓ Check if the COM of the PC is enabled.

4. How to configure the Managed Switch?
   - ✓ The “Hyperterm” is the terminal program in Win95/98/NT. Users can also use any other terminal programs in Linux/Unix to configure the Managed Switch. Please refer to the user guide of that terminal program. But the COM port parameters (baud rate/ data bits/ parity bits/ flow control) must be the same as the setting of the console port of the Managed Switch.

Appendix A
Technical Specifications

Features

- 8 (10/100/1000Mbps) Gigabit Ethernet (TP) switching ports are compliant with IEEE802.3, 802.3u, 802.3z and 802.3ab.
- 16 Gigabit SFP fiber ports.
- Non-blocking store-and-forward shared-memory Web-Smart switched.
- Supports auto-negotiation for configuring speed, duplex mode.
- Supports 802.3x flow control for full-duplex ports.
- Supports collision-based and carrier-based backpressure for half-duplex ports.
- Any ports can be in disable mode, force mode or auto-polling mode.
- Supports Head of Line (HOL) blocking prevention.
- Supports broadcast storm filtering.
- Auto-aging with programmable inter-age time.
- Supports 802.1p Class of Service with 2-level priority queuing.
- Supports port sniffer function
- Programmable maximum Ethernet frame length of range from 1518 to 9216 bytes jumbo frame.
- Supports port-based VLAN, 802.1Q tag-based VLAN.
- Efficient self-learning and address recognition mechanism enables forwarding rate at wire speed.
- Web-based management provides the ability to completely manage the switch from any web browser.
- SNMP/Telnet interface delivers complete in-band management.
- Supports IEEE 802.1d Spanning Tree Protocol.
- Supports IEEE 802.1w Rapid Spanning Trees.
- Supports IEEE 802.1X port-based network access control.
- Supports IP Multicasting to implement IGMP Snooping function.
- Supports 802.1p Class of Service with 2-level priority queuing.
- Supports 802.3ad port trunking with flexible load distribution and failover function.
- Supports ingress port security mode for VLAN Tagged and Untagged frame process.
- Supports SNMP MIB2 and RMON sampling with sampled packet error indication.

Hardware Specifications

- **Standard Compliance:** IEEE802.3/802.3ab / 802.3z / 802.3u / 802.3x
- **Network Interface:**

Configuration	Mode	Connector	Port
10/100/1000Mbps Gigabit TP	NWay	TP (RJ-45)	1 - 8
1000Base-SX Gigabit Fiber	1000 FDX	*SFP	9 - 24
1000Base-LX Gigabit Fiber	1000 FDX	*SFP	9 - 24
1000Base-LX Single Fiber WDM (BiDi)	1000 FDX	*SFP	9 - 24

*Optional SFP module supports LC or BiDi LC transceiver

- **Transmission Mode:** 10/100Mbps support full or half duplex
  1000Mbps support full duplex only
- **Transmission Speed:** 10/100/1000Mbps for TP
  1000Mbps for Fiber
- **Full Forwarding/Filtering Packet Rate:** PPS (packets per second)

Forwarding Rate	Speed
1,488,000PPS	1000Mbps
148,800PPS	100Mbps
14,880PPS	10Mbps

- **MAC Address and Self-learning:** 8K MAC address
  4K VLAN table entries,
- **Buffer Memory:** Embedded 400 KB frame buffer
- **Flow Control:** IEEE802.3x compliant for full duplex
  Backpressure flow control for half duplex
- **Cable and Maximum Length:**

TP	Cat. 5 UTP cable, up to 100m
1000Base-SX	Up to 220/275/500/550m, which depends on Multi-Mode Fiber type
1000Base-LX	Single-Mode Fiber, up to10/30/50Km
1000Base-LX WDM (BiDi)	Single-Mode Single Fiber, up to 20Km

- **Diagnostic LED:**

  System LED : Power, CPU
  Per Port LED:
  10/100/1000M TP Port 1 to 8 : LINK/ACT, SPEED
  1000M SFP Fiber Port 9 to 24 : SFP(LINK/ACT)

- **Power Requirement** **:** AC Line

  Voltage : 100~240 V
  Frequency : 50~60 Hz
  Consumption : 30W
- **Ambient Temperature** **:** 0° to 40°C
- **Humidity** **:** 5% to 90%
- **Dimensions** **:** 44(H) × 442(W) × 209(D) mm
- **Comply with FCC Part 15 Class A & CE Mark Approval**

Management Software Specifications

System Configuration	Auto-negotiation support on 10/100/1000 Base-TX ports, Web browser or console interface can set transmission speed (10/100/1000Mbps) and operation mode (Full/Half duplex) on each port, enable/disable any port, set VLAN group, set Trunk Connection.
Management Agent	SNMP support; MIB II, Bridge MIB, RMON MIB
Spanning Tree Algorithm	IEEE 802.1D
VLAN Function	Port-Base / 802.1Q-Tagged, allowed up to 256 active VLANs in one switch.
Trunk Function	Ports trunk connections allowed
IGMP	IP Multicast Filtering by passively snooping on the IGMP Query.
Bandwidth Control	Supports by-port Egress/Ingress rate control
Quality of Service (QoS)	Referred as Class of Service (CoS) by the IEEE 802.1P standard ,Classification of packet priority can be based on either a VLAN tag on packet or a user-defined Per port QoS. Two queues per port IP TOS Classification TCP/UDP Port Classification IP DiffServe Classification
Port Security	Limit number of MAC addresses learned per port static MAC addresses stay in the filtering table.
Internetworking Protocol	Bridging : 802.1D Spanning Tree IP Multicast : IGMP Snooping IP Multicast Packet Filtering Maximum of 256 active VLANs and IP multicast sessions
Network Management	One RS-232 port as local control console Telnet remote control console SNMP agent : MIB-2 (RFC 1213) Bridge MIB (RFC 1493) RMON MIB (RFC 1757)-statistics VLAN MIB (802.1Q) Web browser support based on HTTP Server and CGI parser TFTP software-upgrade capability.

Note: Any specification is subject to change without notice.

Appendix B
Null Modem Cable Specifications

The DB-9 cable is used for connecting a terminal or terminal emulator to the Managed Switch's RS-232 port to access the command-line interface.

The table below shows the pin assignments for the DB-9 cable.

Function	Mnemonic	Pin
Carrier	CD	1
Receive Data	RXD	2
Transmit Data	TXD	3
Data Terminal Ready	DTR	4
Signal Ground	GND	5
Data Set Ready	DSR	6
Request To Send	RTS	7
Clear To Send	CTS	8

9 Pin Null Modem Cable